

**Lucent Technologies**  
Bell Labs Innovations



***AnyMedia*<sup>®</sup> Access System  
Element Manager for  
Narrowband Services  
Release 1.3**

User Service Manual

363-211-412  
Version 1.00  
(08.99)

**Copyright © 1999 Lucent Technologies. All rights reserved.  
Printed in U.S.A.**

This material is protected by the copyright and trade secret laws of the United States and other countries. It may not be reproduced, distributed or altered in any fashion by any entity, (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts or licensing, without the express written consent of the Customer Training and Information Products organization and the business management owner of the material.

**Notice**

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

**Ordering Information**

The order number for this document is 363-211-412. For more ordering information, refer to "How to Order Documents" in the section "About This Document".

**How to Comment on This Document**

A feedback form is located immediately after the legal page of this document. Please send or fax your comments and suggestions to:

Lucent Technologies Network Systems GmbH  
Fax no.: +49 911 526-3545

**Trademarks**

*Acrobat Reader* is registered trademark of Adobe Systems Incorporated.

*AnyMedia* is a trademark of Lucent Technologies.

*Internet Explorer* is a copyright of Microsoft Corporation.

*Netscape Navigator* is a trademark of Netscape Communications Corporation.

*Windows 95* and *Windows 98* are copyrights of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

**Quality Management System**

The Quality Management System (QMS) for Lucent Technologies' Product Realization Center (PRC) Access has been registered to ISO 9001 under the Norwegian Scheme by Det Norske Veritas (DNV) since June 1993. ISO 9001 is an international quality standard recognized by more than 90 countries worldwide. It is a model for quality assurance in design, development, production, installation, and servicing.

# How Are We Doing?

Telefax to:  
Lucent Technologies Network Systems GmbH  
Fax no.: +49 911 526-3545

Lucent Technologies welcomes your feedback on this document. Your comments can be of great value in helping us improve our documentation. Please use a copy of this page for your comments.

1. Please rate the effectiveness of this document in the following areas:

	Excellent	Good	Fair	Poor
Ease of Use				
Clarity				
Completeness				
Accuracy				
Organization Structure				
Appearance				
Examples				
Illustrations				
Overall Satisfaction				

2. Please check the ways you feel we could improve this document:

- ☐ Improve the overview/introduction
- ☐ Improve the tables of contents
- ☐ Improve the organization structure
- ☐ Include more figures
- ☐ Add more examples
- ☐ Add more detail
- ☐ Make it more brief/concise
- ☐ Add more step-by-step procedures/tutorials
- ☐ Add more troubleshooting information
- ☐ Make it less technical
- ☐ Add more/better quick reference aids
- ☐ Improve the index

Please provide details for the suggested improvement:

.....

.....

.....

3. What did you like most about this document?

.....

.....

.....

4. Feel free to write any comments below or on an attached sheet.

.....

.....

.....

.....

.....

If we may contact you concerning your comments, please complete the following:

Name: ..... Telephone Number: .....

Company/Organization: ..... Date: .....

Address: .....

When you have completed this form, please fax it to the address on top of this page.



---

# Contents

---

<b>About this Document</b>	<a href="#"><u>XI</u></a>
1 Overview	<a href="#"><u>XI</u></a>
2 Intended Audience	<a href="#"><u>XII</u></a>
3 How to use this document	<a href="#"><u>XIII</u></a>
4 Conventions Used	<a href="#"><u>XIV</u></a>
6 General Safety Information	<a href="#"><u>XV</u></a>
6.1 General Notes on Safety	<a href="#"><u>XV</u></a>
6.2 General Safety Requirements	<a href="#"><u>XVI</u></a>
7 Related Documentation	<a href="#"><u>XVIII</u></a>
7.1 Print Copy (Hard Copy)	<a href="#"><u>XVIII</u></a>
7.2 CD-ROM	<a href="#"><u>XIX</u></a>
8 How to Order This Document	<a href="#"><u>XIX</u></a>
9 How to Comment on This Document	<a href="#"><u>XX</u></a>

---

<b>1 Functional Description</b>	<a href="#"><u>1-1</u></a>
1.1 About this Subject	<a href="#"><u>1-1</u></a>
1.2 Introduction	<a href="#"><u>1-2</u></a>
1.2.1 Main Functions	<a href="#"><u>1-2</u></a>
1.2.2 ISO Functional Areas	<a href="#"><u>1-3</u></a>
1.2.3 Applications	<a href="#"><u>1-4</u></a>
1.2.4 System Working Modes	<a href="#"><u>1-5</u></a>
1.3 System and Software Architecture	<a href="#"><u>1-7</u></a>
1.3.1 Functional Groups	<a href="#"><u>1-7</u></a>
1.3.2 Hardware Platform	<a href="#"><u>1-17</u></a>
1.4 Working with AEM-NB	<a href="#"><u>1-19</u></a>
1.4.1 Network Planning and Physical Installation	<a href="#"><u>1-20</u></a>
1.4.2 Configuration Management	<a href="#"><u>1-21</u></a>
1.4.3 Network Operation & Surveillance	<a href="#"><u>1-22</u></a>
1.4.4 System Security and User Groups	<a href="#"><u>1-27</u></a>
1.5 Network Configuration	<a href="#"><u>1-28</u></a>
1.5.1 AEM-NB Server without Clients and external OS (LAN)	<a href="#"><u>1-28</u></a>

---

## Contents

1.5.2	AEM-NB Server with Clients and without external OS (LAN)	<a href="#">1-29</a>
1.5.3	AEM-NB Server without Clients and with external OS (WAN)	<a href="#">1-30</a>
1.5.4	AEM-NB Server with Clients and external OS (WAN)	<a href="#">1-31</a>

---

<b>2</b>	<b>Software Installation and Commissioning</b>	<a href="#">2-1</a>
2.1	General	<a href="#">2-1</a>
2.1.1	Introduction	<a href="#">2-2</a>
2.2	Installation Procedure	<a href="#">2-6</a>
2.2.1	Full Installation	<a href="#">2-6</a>
2.2.2	Installing Individual Packages	<a href="#">2-40</a>
2.2.3	Cancel Installation	<a href="#">2-43</a>
2.2.4	Remove <i>AnyMedia</i> Package Installations	<a href="#">2-43</a>

---

<b>3</b>	<b>System Management</b>	<a href="#">3-1</a>
3.1	Overview	<a href="#">3-1</a>
3.2	System Access	<a href="#">3-2</a>
3.2.1	Login to Operation System	<a href="#">3-2</a>
3.2.2	Logout from Operation System	<a href="#">3-3</a>
3.2.3	AEM-NB Access Bar	<a href="#">3-4</a>
3.2.4	Capacity	<a href="#">3-5</a>
3.3	General Information on Keyboard and Windows	<a href="#">3-6</a>
3.3.1	Keyboard	<a href="#">3-6</a>
3.3.2	Mouse	<a href="#">3-6</a>
3.3.3	Different Aspects of the Cursor	<a href="#">3-7</a>
3.3.4	Basics on Windows	<a href="#">3-7</a>
3.3.5	Window Menu	<a href="#">3-10</a>
3.3.6	Menu Bar	<a href="#">3-11</a>
3.3.7	Cursor Menu	<a href="#">3-11</a>
3.3.8	Workspace Manager	<a href="#">3-12</a>
3.3.9	Workspace Menu	<a href="#">3-12</a>
3.3.10	Controls in AEM-NB Windows	<a href="#">3-13</a>
3.4	Application Start-Up and Shutdown	<a href="#">3-17</a>

---

## Contents

3.4.1	General on Applications	<a href="#">3-17</a>
3.4.2	AEM-NB Server Applications	<a href="#">3-18</a>
3.4.3	Start-Up/Shutdown of Server Applications via GUI	<a href="#">3-18</a>
3.4.4	Start-Up/Shutdown of Server Applications via Command Line	<a href="#">3-20</a>
3.4.5	Deinstall AEM-NB from Your System	<a href="#">3-20</a>
3.5	Print out Reports	<a href="#">3-21</a>
3.6	Backup and Restore	<a href="#">3-23</a>
3.6.1	Basics on Backups and AEM-NB Databases	<a href="#">3-23</a>
3.6.2	Commands for Backup, Archive and Restore	<a href="#">3-24</a>
3.6.3	Backup, Archive and Restore Procedures	<a href="#">3-26</a>
3.6.4	Examples for Backup Schedules	<a href="#">3-28</a>
3.7	Log Management	<a href="#">3-31</a>
3.7.1	Different Log Types	<a href="#">3-31</a>
3.7.2	Configuration of Logs	<a href="#">3-31</a>
3.7.3	Log Viewer Window	<a href="#">3-32</a>
3.8	Disaster Recovery	<a href="#">3-37</a>

---

<b>4</b>	<b>User Management</b>	<a href="#">4-1</a>
4.1	Introduction	<a href="#">4-1</a>
4.2	User	<a href="#">4-2</a>
4.2.1	Create User	<a href="#">4-2</a>
4.2.2	Modify User	<a href="#">4-4</a>
4.2.3	Delete User	<a href="#">4-6</a>
4.3	Domains	<a href="#">4-8</a>
4.3.1	Create Domains	<a href="#">4-8</a>
4.3.2	Modify Domains	<a href="#">4-11</a>
4.3.3	Delete Domains	<a href="#">4-14</a>
4.4	User Groups	<a href="#">4-16</a>
4.4.1	Create User Groups	<a href="#">4-16</a>
4.4.2	Modify User Groups	<a href="#">4-21</a>
4.4.3	Delete User Groups	<a href="#">4-26</a>
4.5	Controlled Objects	<a href="#">4-29</a>
4.5.1	Modify Controlled Objects	<a href="#">4-29</a>

---

# Contents

---

<b>5</b>	<b>Configuration Management/Provisioning</b>	<b><a href="#">5-1</a></b>
5.1	Overview	<a href="#">5-1</a>
5.1.1	Overview of <i>AnyMedia</i> Access System R1.3	<a href="#">5-1</a>
5.1.2	Synchronization Interfaces	<a href="#">5-3</a>
5.1.3	OAM&P Interfaces	<a href="#">5-4</a>
5.1.4	Alarm Interfaces	<a href="#">5-4</a>
5.1.5	Testing Interfaces	<a href="#">5-4</a>
5.1.6	Plug & Play Capabilities	<a href="#">5-5</a>
5.2	Configuration Manager Window	<a href="#">5-7</a>
5.2.1	Network Browser	<a href="#">5-8</a>
5.2.2	Menu Bar	<a href="#">5-9</a>
5.2.3	Status Bar	<a href="#">5-11</a>
5.2.4	Cursor Menu	<a href="#">5-12</a>
5.3	Equipment Configuration	<a href="#">5-14</a>
5.3.1	Add a Network Element	<a href="#">5-17</a>
5.3.2	Shelf View	<a href="#">5-22</a>
5.3.3	Edit/View of Configuration Data	<a href="#">5-45</a>
5.3.4	Network Element Software Upgrade	<a href="#">5-65</a>
5.3.5	Nonvolatile Data Storage (NVDS)	<a href="#">5-70</a>
5.3.6	Network Element Reset	<a href="#">5-73</a>
5.3.7	TL1 Cut-Through	<a href="#">5-74</a>
5.3.8	Delete Network Element	<a href="#">5-75</a>
5.4	Service Provisioning	<a href="#">5-77</a>
5.4.1	Create a V5 Network Interface	<a href="#">5-83</a>
5.4.2	Add V5 Links to V5 Interface	<a href="#">5-94</a>
5.4.3	Add Primary V5.2 Links	<a href="#">5-109</a>
5.4.4	Add Secondary V5.2 Link	<a href="#">5-111</a>
5.4.5	Add V5 User Port	<a href="#">5-114</a>
5.4.6	V5 Signalling	<a href="#">5-132</a>
5.4.7	Move a V5 Interface in Service	<a href="#">5-153</a>
5.4.8	Move a V5 Link in Service	<a href="#">5-154</a>
5.4.9	Move a V5 User Port in Service	<a href="#">5-154</a>
5.4.10	Delete V5 User Port	<a href="#">5-155</a>
5.4.11	Delete V5 Link	<a href="#">5-155</a>
5.4.12	Remove Communication Channel	<a href="#">5-156</a>



---

## Contents

5.4.13	Remove Communication Path	<a href="#">5-157</a>
5.4.14	Remove Primary Link	<a href="#">5-157</a>
5.4.15	Remove Secondary Link	<a href="#">5-158</a>
5.4.16	Remove V5 Protection Group 2	<a href="#">5-158</a>
5.4.17	Delete V5 Interface	<a href="#">5-159</a>

---

<b>6</b>	<b>Fault Management and Maintenance</b>	<a href="#">6-1</a>
6.1	Overview	<a href="#">6-1</a>
6.2	Alarm Management	<a href="#">6-1</a>
6.2.1	Overview	<a href="#">6-1</a>
6.2.2	Maintain Up-To-Date Alarm Information	<a href="#">6-2</a>
6.2.3	Alarm Notification to the User	<a href="#">6-3</a>
6.2.4	Provide Access to the Current Alarm Data	<a href="#">6-7</a>
6.2.5	Managing the Raising of Alarms	<a href="#">6-7</a>
6.2.6	Manage Alarm Acknowledgment	<a href="#">6-8</a>
6.2.7	Managing the Clearing of Alarms	<a href="#">6-8</a>
6.2.8	Alarm Data Synchronization	<a href="#">6-8</a>
6.2.9	AEM-NB Alarm Log Handling	<a href="#">6-9</a>
6.2.10	Periodical Deletion of Cleared Alarms	<a href="#">6-9</a>
6.3	Alarm Monitoring	<a href="#">6-10</a>
6.3.1	General	<a href="#">6-10</a>
6.3.2	Starting and Terminating the Alarm Viewer	<a href="#">6-10</a>
6.3.3	Performing Alarm Viewer Functions	<a href="#">6-11</a>
6.3.4	System Management Functions	<a href="#">6-18</a>
6.3.5	Alarm Viewer Functions	<a href="#">6-21</a>
6.4	Test Management	<a href="#">6-23</a>
6.4.1	User Line Test	<a href="#">6-25</a>
6.4.2	User Port Test	<a href="#">6-29</a>
6.4.3	Standby Card Test Scheduling	<a href="#">6-31</a>
6.4.4	Built-in Self-Test	<a href="#">6-32</a>
6.4.5	TAP-Test	<a href="#">6-33</a>
6.4.6	CRC Test	<a href="#">6-34</a>
6.4.7	Loopback Test at the Feeder Side	<a href="#">6-37</a>
6.4.8	Loopback Test at the ISDN User Port Side	<a href="#">6-38</a>

---

## Contents

6.5	Information Management and Maintenance	<a href="#">6-40</a>
6.5.1	NE-AEM-NB Connection States	<a href="#">6-40</a>
6.5.2	Changing Connection States	<a href="#">6-40</a>
6.5.3	Configuration Data Synchronization after Association	<a href="#">6-41</a>
6.5.4	Alarm Data Synchronization after Association	<a href="#">6-42</a>
6.5.5	Association Maintenance	<a href="#">6-43</a>
6.6	Alarms	<a href="#">6-44</a>
6.6.1	Overview	<a href="#">6-44</a>
6.6.2	Alarm Types	<a href="#">6-44</a>
6.6.3	Network Element Alarms	<a href="#">6-46</a>
6.6.4	Element Manager Platform Alarms	<a href="#">6-46</a>

---

<b>A</b>	<b>Data Communications Network (DCN) Configuration</b>	<a href="#">A-1</a>
A.1	Overview	<a href="#">A-1</a>
A.2	DCN Introduction	<a href="#">A-1</a>
A.3	Terms Used in this Chapter	<a href="#">A-2</a>
A.4	Network Element Communication Capabilities	<a href="#">A-2</a>
A.5	AEM-NB Communication Capabilities	<a href="#">A-5</a>
A.6	Recommended DCN Configurations	<a href="#">A-5</a>
A.6.1	ROC Over Permanent Leased Lines DCN	<a href="#">A-5</a>
A.6.2	Communication with Remote NEs Using Inband ATM PVC	<a href="#">A-10</a>

---

<b>B</b>	<b>System Variables and Configuration Parameters</b>	<a href="#">B-1</a>
B.1	Overview	<a href="#">B-1</a>
B.2	System Variables	<a href="#">B-1</a>
B.3	Configuration Parameters	<a href="#">B-2</a>
B.3.1	<i>AnyMedia</i> Server Configuration Parameters	<a href="#">B-2</a>
B.3.2	<i>AnyMedia</i> Client GUI Configuration Variables	<a href="#">B-4</a>

---

# Contents

---

<b>C</b>	<b>Northbound Interface</b>	<a href="#"><u>C-1</u></a>
C.1	Overview	<a href="#"><u>C-1</u></a>
C.2	Northbound Interface Basics	<a href="#"><u>C-1</u></a>
C.2.1	Northbound Interface Description	<a href="#"><u>C-1</u></a>
C.3	Northbound Interface Specific TL1 Messages	<a href="#"><u>C-3</u></a>
C.3.1	REPT ALM (Report Alarm)	<a href="#"><u>C-4</u></a>
C.3.2	RTRV-ALM (Retrieve-Alarms)	<a href="#"><u>C-9</u></a>
C.3.3	RTRV-ALM-ENV (Retrieve-Alarm-Environment)	<a href="#"><u>C-15</u></a>

---

<b>AB</b>	<b>Abbreviations</b>	<a href="#"><u>AB-1</u></a>
-----------	----------------------	-----------------------------

---

<b>GL</b>	<b>Glossary</b>	<a href="#"><u>GL-1</u></a>
-----------	-----------------	-----------------------------

---

<b>IN</b>	<b>Index</b>	<a href="#"><u>IN-1</u></a>
-----------	--------------	-----------------------------

---

# Contents

---

# About this Document

---

## 1 Overview

---

### Purpose

This User Service Manual (USM) provides the following information for Lucent Technologies *AnyMedia*® Access System Element Manager for Narrowband Services (AEM-NB), Release 1.3:

- A product overview and a functional product description
- System turn-up procedures and system modifications
- User Management
- Configuration management
- Fault Management, Maintenance.

The purpose of the USM is to provide the provisioning personnel with all information necessary to provision an *AnyMedia* Access System R1.3 via the AEM-NB.

The USM is a network oriented manual and will be shipped to all sites where an AEM-NB is available. It provides the provisioning operator(s) with necessary information to configure or re-configure network elements after local installation.

The philosophy behind the provisioning of network elements within a network is that the network is already installed, configured and service has been provided to the network after first installation and that re-configuration of the NE is necessary. Provisioning takes place from the AEM-NB, located in one or more central offices.

## **2 Intended Audience**

---

The USM is intended for personnel who take care of deploying NEs by carrying out all provisioning activities of the NEs using the AEM-NB.

Tasks to be performed by the Provisioning personnel are:

- Collect information of provisioning data (e.g. check shelf layout, units list)
- Put ports in-service and out-service
- Assign timeslots (Cross Connections)
- Download and upload the provisioning data to and from the NEs
- Testing of assigned ports.
- Recognize, interpret, analyze or correct failures, caused by provisioning data that is configured incorrectly.

The personnel should at least have the following education level:

- Computer knowledge (e.g. windows applications and/or SUN applications)
- Telecommunication Network knowledge.

## 3 How to use this document

---

The guide is divided into a number of sections (subjects), clearly separated by numbered tabs. The front pages of the guide also describe this division, and list the titles of the subjects together with the corresponding tab numbers. Through this readers can quickly select the subject of their interests and needs.

- **How are we doing**  
A comment form so readers can give feedback to improve the next revision of the document.
- **Table of contents, list of figures, list of tables**
- **Overview**  
Defines the purpose of the document and the intended audience. Also included are topics about the conventions used in the document, related documentation, how to order documents, and how to comment on this document.
- **Chapter 1, Functional Description**  
Contains a short overview over the system, its features and capabilities.
- **Chapter 2, Software Installation**  
Describes the standard procedure to install the AEM-NB R1.3 server package (server applications) and client package (client applications).
- **Chapter 3, System Management**  
Provides the system administrator with all information necessary to administer the AEM-NB so that it can be used as a centralized management system.
- **Chapter 4, User Management**  
Describes all actions necessary to create/modify/delete users, user groups and domains and the handling of controlled objects.
- **Chapter 5, Configuration Management, Provisioning**  
Describes the database and software management, the default system configuration parameters and the provisioning and service activation, the inventory management, clock synchronization management and protection switching.
- **Chapter 6, Fault Management/Maintenance**  
Describes alarms and events, how to use the Alarm Viewer, how to perform tests and trouble clearing procedures.
- **Appendix A**  
Describes the Data Communications Network (DCN) configurations.
- **Appendix B**  
Provides information about the system variables and the configuration parameters.
- **Appendix C**  
Describes the TL1 Northbound Interface.
- **Abbreviations and Acronyms**  
Lists all abbreviations and acronyms used in this manual.

- **Glossary**  
Defines special terms used in this manual.
- **Index**  
Alphabetical index to quickly search for paragraphs in the manual which provide more information on a certain keyword.

## 4 Conventions Used

---

The following are terms used in this USM that may have a different meaning than the general or common use of the term.

- In the AEM-NB, the term *access* means that the system provides the primary service interface for the customer to enter the network.
- The term *plug-in* is generally used for circuit pack units (COMDAC, CIU, IO-E1, HDLC and application packs (APs)) which have pre-designated slots with the capability to plug-in the circuit pack.

<b>Numbering</b>	<p>Each fascicle can be identified by its number and contains a chapter which is numbered accordingly (e.g. Chapter 2 is contained in Fascicle 2).</p> <p>The page, figure and table numbering begins with “1” in every chapter. To be able to identify them easily, these numbers are prefixed with the fascicle number. For example, Figure 2-3 designates the third figure in Fascicle 2.</p>
<b>Cross-References</b>	<p>Cross-reference conventions are identical with those used for numbering, i.e. the first number in cross-references refers to the corresponding fascicle.</p>
<b>Keyword Blocks</b>	<p>To facilitate the location of specific text passages, the guide contains so-called keyword blocks. These are placed to the left of the main text and contain either a keyword or a word which indicates the contents of a paragraph or group of paragraphs.</p>
<b>Abbreviations</b>	<p>Each abbreviation used in this guide is listed in Fascicle AB (“Abbreviations”) of the hardcopy version unless it can be assumed that the reader is familiar with this abbreviation.</p>
<b>Commands</b>	<p>Commands and messages are displayed in <code>constant-width</code> font (e.g., <code>tar xf /cdrom/cdrom_name/AnyMediaEMSR10.tar</code>).</p>
<b>Trademarks</b>	<p>The trademarks used in this document are identified after the title page. Trademarks of Lucent Technologies and other companies are in italics and the trademarks modify a noun (e.g., the system name contains a trademark, <i>AnyMedia</i>™ Access System). A trademark is not treated as an acronym (it is not spelled out or expanded).</p>
<b>Lucent Technologies trademarks</b>	<p>Lucent Technologies trademarks are identified with the registered mark (®) or trademark (™) symbol the first time the trademarks are used in a chapter.</p>
<b>Trademarks of other companies</b>	<p>The trademarks of other companies are identified with a footnote reference the first time the trademarks are used in a chapter.</p>



**Typographical conventions**

The following table gives examples of the typographical conventions used in this chapter.

**Table 0-5    Typographical Conventions**

Object	Example	Meaning
Keyboard	<b>Return</b> or <b>A</b>	<b>Return</b> or <b>A</b> key on the keyboard
	<b>Shift-Ctrl-B</b>	<b>Shift</b> , <b>Ctrl</b> and <b>B</b> key pressed simultaneously
	<b>Esc A B</b>	<b>Esc</b> , <b>A</b> and <b>B</b> key pressed one after the other
Pushbutton	<b>Apply</b>	<b>Apply</b> pushbutton in a window
Menu	<b>File -&gt; Exit</b>	Menu option <b>Exit</b> in <b>File</b> menu
Objects in windows	<b>Date</b>	Designates the object <b>Date</b> in a window (e.g. text field, check box, spin box etc.)

---

## 6        General Safety Information

This section lists the safety information needed for the *AnyMedia* Access System for system turn-up after installation has been completed, operating, provisioning and maintaining the system.

---

### 6.1        General Notes on Safety

This system has been developed in line with the present state-of-the-art and fulfils the current national and international safety requirements. It is provided with a high degree of operational safety resulting from many years of development experience and continuous stringent quality checks in our company.

The system is safe in normal operation. There are, however, some potential sources of danger that cannot be completely eliminated. In particular, these arise during the

- Opening of housings or equipment covers
- Manipulation of any kind within the equipment, even if it has been disconnected from the power supply
- Disconnection of optical or electrical connections

through possible contact with

- Live parts
- Laser light
- Hot surfaces
- Sharp edges, or
- Devices sensitive to electrostatic discharge.

## 6.2 General Safety Requirements

---

In order to keep the technically unavoidable residual risk to a minimum, it is imperative to observe the following rules:

- **Installation, configuration and disassembly must be carried out only by expert personnel and with reference to the respective documentation.**  
Due to the complexity of the unit/system, the personnel requires special training.
- **The unit/system must be operated by expert and authorized users only.**  
The user must operate the unit/system only after having read and understood the chapter on safety and the parts of the documentation relevant to operation. For complex systems, additional training is recommended. Any obligatory training for operating and service personnel must be carried out and documented.
- **Any conversions or changes to the system or parts of the system (including the software) must be carried out by qualified Lucent Technologies personnel or by expert personnel authorized by Lucent Technologies.**  
All changes carried out by other persons lead to a complete exemption from liability.  
No components/spare parts must be used other than those recommended by the manufacturer and those listed in the procurement documents.
- **The unit/system must not be operated unless it is in perfect working order.**  
Any faults and errors that might affect safety must be reported immediately by the user to a person in responsibility.
- **The equipment must be supplied with Safety Extra-Low Voltage (SELV) of -48 V and the positive terminal of this source must be correctly connected to the protective earth.**  
Never connect to -60 V.
- **The unit/system must be operated only with the connections and under the environmental conditions as described in the documentation.**
- **The removal or disabling of safety facilities, the clearing of faults and errors, and the maintenance of the equipment must be carried out by specially qualified personnel only.**  
**The respective parts of the documentation must be strictly observed.**  
The documentation must also be consulted during the selection of measuring and test equipment.
- **Transport, storage and operation of the unit/system must be under the permissible conditions only.**  
See accompanying documentation and information on the unit/system.
- **Calibrations, special tests after repairs and regular safety checks must be carried out, documented and archived.**
- **Only use tested and virus-free diskettes.**

- **Do not place the shelves on an unstable cart, stand, or table.**  
The product may fall causing serious damage to the equipment.
- **Never push objects of any kind into this product through cabinet slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electrical shock. Never spill liquid of any kind on the product.**

### 6.2.1 Safety Symbols and Labels

All safety instructions have a uniform appearance. They include a *signal word* that classifies the danger and a *text block* that contains descriptions of the type and cause of the danger, the consequences of ignoring the safety instruction and the measures that can be taken to minimize the danger. In some safety instructions, a *warning symbol* is placed underneath the signal word.

#### Classification

There are five classes of safety instructions: “Danger”, “Warning”, “Caution”, “Important” and “Notice”. The classification is shown in the following table.

<b>DANGER</b>	Serious injury is definite or likely.
<b>WARNING</b>	Serious injury is possible.
<b>CAUTION</b>	Minor injury is definite, likely or possible, or material damage to the product or in the product environment is definite or likely.
<b>IMPORTANT</b>	Material damage to the product or in the product environment is possible.
<b>NOTICE</b>	A fault, i.e. considerable impairment to operation, will be caused or may be caused.

## 7 Related Documentation

---

**Document list**            The following is related documentation for the AEM-NB and for additional components:

**Table 1      List of Documents**

<b>Component</b>	<b>Manual Type</b>	<b>Comcode</b>	<b>CIC Ordering Number</b>
<i>AnyMedia</i> Access System	Applications, Planning, and Ordering Guide (APOG)	108 298 670	363-211-110 <sup>a</sup>
<i>AnyMedia</i> Access System	Command and Message Manual (CMM)	108 298 761	363-211-111 <sup>a</sup>
<i>AnyMedia</i> Access System	User Service Manual (USM) Vol. 1 (Narrowband Services)	108 298 811	363-211-112 <sup>a</sup>
<i>AnyMedia</i> Access System	User Service Manual (USM) Vol. 2 (Broadband Services)	108 543 380	363-211-115 <sup>a</sup>
<i>AnyMedia</i> Access System	Installation Manual (IM) (For Rack Configurations)	108 298 779	363-211-113 <sup>a</sup>
Mass Provisioning Tool for V5 Services	User Manual		363-211-116 <sup>b</sup>
AEM-NB R1.3	Functional Description		363-211-411 <sup>a</sup>

a For the ordering address see Chapter 8, How to Order This Document.

b The MPT User Manual is included in the Mass Provisioning Tool delivery. Additionally it is available in PDF format on CD-ROM.

### 7.1 Print Copy (Hard Copy)

---

**Document packaging and format**            All listed documents are available in print.

## 7.2 CD-ROM

---

The User Service Manual and the Functional Description are available in PDF format on CD-ROM and an Adobe Acrobat Reader<sup>1</sup> is provided to view them.

**Table 2 Customer Documentation on CD-ROM**

Component	CD-ROM	Ordering Number
AEM-NB R1.3	Customer Documentation on CD-ROM includes: <ul style="list-style-type: none"><li>– User Service Manual (USM)</li><li>– Functional Description</li></ul>	363-211-415

## 8 How to Order This Document

---

**Ordering number** The ordering number for the AEM-NB *User Service Manual* is 363-211-412.

**Order procedure** To order additional hard copies of this document and/or to request placement on the standing order list, send or call in an order as follows:

Mail Order <sup>a</sup>	Telephone Order (Monday through Friday)
Lucent Technologies Customer Information Center Attention: Priscilla Stanley, email: pfstanley@lucent.com 2855 N. Franklin Road P.O. Box 19901 USA-Indianapolis, IN 46219	Within USA: 1-888-LUCENT8 7:30 a.m. to 6:30 p.m. EST FAX from USA: +1-800-566-9568 FAX Worldwide: +1-317-322-6699

<sup>a</sup> For ordering, a purchase order number, or charge card number is required with all orders. Make checks payable to Lucent Technologies.

**One-time orders** One-time orders include the contents for the current document issue in effect at the time of order.

**Standing orders** You may request an update on the standing order list for all later reissues of any document. The standing order list for each document provides automatic distribution for all reissues of the document.

---

<sup>1</sup> *Acrobat Reader* is a registered trademark of Adobe Systems Incorporated.

## 9      **How to Comment on This Document**

---

### **Document comment procedure**

The first sheet in this manual (after the title page) is the feedback form *How Are We Doing?*

Please use this form to fax your comments and suggestions concerning the USM, 363-211-412 to:

Lucent Technologies Network Systems GmbH  
Fax no.: +49 911 526-3545.

---

## Contents

<b>1.1</b>	<b>About this Subject</b>	<a href="#"><u>1-1</u></a>
<b>1.2</b>	<b>Introduction</b>	<a href="#"><u>1-2</u></a>
1.2.1	Main Functions	<a href="#"><u>1-2</u></a>
1.2.2	ISO Functional Areas	<a href="#"><u>1-3</u></a>
1.2.2.1	Configuration Management	<a href="#"><u>1-3</u></a>
1.2.2.2	Fault Management	<a href="#"><u>1-3</u></a>
1.2.2.3	Performance Management	<a href="#"><u>1-4</u></a>
1.2.2.4	Security Management	<a href="#"><u>1-4</u></a>
1.2.3	Applications	<a href="#"><u>1-4</u></a>
1.2.4	System Working Modes	<a href="#"><u>1-5</u></a>
<b>1.3</b>	<b>System and Software Architecture</b>	<a href="#"><u>1-7</u></a>
1.3.1	Functional Groups	<a href="#"><u>1-7</u></a>
1.3.1.1	NE Management	<a href="#"><u>1-8</u></a>
1.3.1.2	General Components	<a href="#"><u>1-12</u></a>
1.3.1.3	Software Platform	<a href="#"><u>1-14</u></a>
1.3.1.3.1	Software Bus	<a href="#"><u>1-14</u></a>
1.3.1.3.2	Repository	<a href="#"><u>1-14</u></a>
1.3.1.4	Graphical User Interface (GUI)	<a href="#"><u>1-15</u></a>
1.3.1.5	Northbound Interface	<a href="#"><u>1-16</u></a>
1.3.1.6	Southbound Interface	<a href="#"><u>1-16</u></a>
1.3.2	Hardware Platform	<a href="#"><u>1-17</u></a>
1.3.2.1	Architecture	<a href="#"><u>1-17</u></a>
1.3.2.2	Requirements	<a href="#"><u>1-18</u></a>
<b>1.4</b>	<b>Working with AEM-NB</b>	<a href="#"><u>1-19</u></a>
1.4.1	Network Planning and Physical Installation	<a href="#"><u>1-20</u></a>

---

# Contents

1.4.2	Configuration Management	<a href="#">1-21</a>
1.4.3	Network Operation & Surveillance	<a href="#">1-22</a>
1.4.3.1	Fault Management	<a href="#">1-22</a>
1.4.3.1.1	Fault Identification	<a href="#">1-23</a>
1.4.3.1.2	Fault Localisation and Diagnosis	<a href="#">1-24</a>
1.4.3.1.3	Fault Clearance	<a href="#">1-24</a>
1.4.3.2	Network Modification	<a href="#">1-25</a>
1.4.3.2.1	Installation and Removal of an NE	<a href="#">1-25</a>
1.4.3.2.2	Modification of NEs	<a href="#">1-26</a>
1.4.3.3	Performance Monitoring	<a href="#">1-26</a>
1.4.4	System Security and User Groups	<a href="#">1-27</a>
<b>1.5</b>	<b>Network Configuration</b>	<a href="#">1-28</a>
1.5.1	AEM-NB Server without Clients and external OS (LAN)	<a href="#">1-28</a>
1.5.2	AEM-NB Server with Clients and without external OS (LAN)	<a href="#">1-29</a>
1.5.3	AEM-NB Server without Clients and with external OS (WAN)	<a href="#">1-30</a>
1.5.4	AEM-NB Server with Clients and external OS (WAN)	<a href="#">1-31</a>



---

**1.1 About this Subject**

---

<b>Scope</b>	This chapter describes the <i>AnyMedia</i> ® Access System Element Manager for Narrowband Services (AEM-NB) R1.3. This release is compatible with the network element (NE) R1.3.
<b>Purpose</b>	This chapter provides an overview of the AEM-NB and tries to give an insight into the functioning of the AEM-NB by providing detailed information on the AEM-NB features mentioned.
<b>Contents</b>	<p>The following AEM-NB subjects are described:</p> <ul style="list-style-type: none"><li>■ Basic functionality</li><li>■ Management features</li><li>■ System and software architecture</li><li>■ Hardware and software platform</li><li>■ Interfaces</li><li>■ Applications.</li></ul>

## 1.2 Introduction

---

<b>General</b>	The AEM-NB is part of a Telecommunication Management Network (TMN). It represents the element management layer and fulfils the tasks of the ISO ( <i>International Standardizations Organisation</i> ) functional areas (see Chapter 1.2.2, page 1-3).
<b>Benefits</b>	<p>This provides some benefits for the operator:</p> <ul style="list-style-type: none"><li>■ Better control over revenue generating services by local and centralized management</li><li>■ Reduced time and effort for provisioning tasks</li><li>■ Fast and efficient fault detection and isolation</li><li>■ Prevention of unauthorized access by appropriate security mechanisms</li><li>■ Reduction of operator mistakes by easy-to-use Graphical User Interface (GUI)</li><li>■ Integration with higher management levels for network, service and business purposes.</li></ul>

### 1.2.1 Main Functions

---

The AEM-NB provides the following main characteristics/functions:

- Support of all *AnyMedia* Access Systems features
- Equipment Overview
- Common alarm handling for all network elements (NEs)
- Report, Log, Backup & Restore functions
- TL1 NE access via TCP/IP based on DCN
- User security handling (user profiles, NE domains)
- Online Help
- Multi User access
- Northbound interfaces (TL1).

---

## **1.2.2 ISO Functional Areas**

---

### **1.2.2.1 Configuration Management**

The Configuration Management supports the complete range of graphical functions to provision and maintain the R1.3 NEs. Network topologies, shelf views and self-explaining menus are navigating the operator to configure POTS, ISDN-BRA and Leased Line Services (no provisioning can be done for leased lines). The following main functionalities are offered (for more detail see Chapter 1.3.1.1, page 1-8):

- Inventory management
- Equipment provisioning and maintenance
- Service provisioning
- Clock synchronization
- System/Equipment/Service status
- Software download
- NE database backup and restore
- System date/time synchronization.

### **1.2.2.2 Fault Management**

The Fault Management supports the operator in detecting, displaying, localizing and logging any faults occurring in the managed network. The following main functionalities are offered (for more detail see Chapter 1.3.1.1, page 1-8):

- Handling of alarm severities (critical, major, minor)
- Receiving of autonomous alarm messages
- Retrieving of alarms per NE, plug-in, application pack
- Retrieving of alarm and event logs from NE
- Initialization of tests for fault analysis purposes.

### 1.2.2.3 Performance Management

The Performance Management provides facilities for retrieving, storing as logs and printing the logs of the NE performance data to ensure the quality of service.

### 1.2.2.4 Security Management

The Security Management functions which are based on UNIX<sup>®1</sup> control the access to the AEM-NB and to the managed NEs. The following main functionalities are offered (for more detail see Chapter 1.3.1.1, page 1-8):

- AEM-NB user administration
- AEM-NB user security profile
- No additional NE login for current AEM-NB user
- AEM-NB access via login name and password<sup>2</sup>
- Inactivity user session time-out<sup>2</sup>.

## 1.2.3 Applications

---

The AEM-NB provides 6 applications which give access to the management functionality as described in Chapter 1.2.2, page 1-3. The following applications are available:

- System Administration
- User Administration and Profiling
- Log Viewer
- Alarm Viewer
- Configuration Manager
- BroadBand EM.

Each application is composed by one or more tasks. The default user group assignment to the individual applications/tasks is described in Chapter 1.4.4, page 1-27.

---

1 UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

2 provided by the SUN Solaris operation system.

### 1.2.4 System Working Modes

The AEM-NB can work in the following two modes:

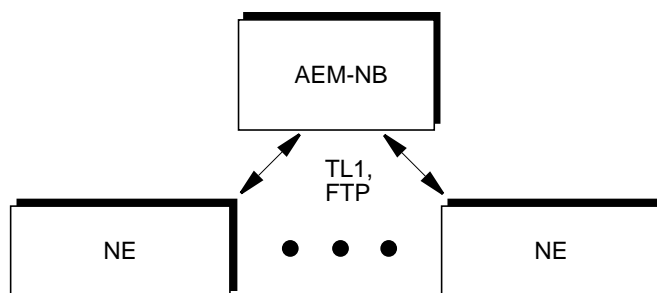
- Stand-alone mode
- Integrated management mode.

These modes are not mutually exclusive, i.e. the AEM-NB is always able to perform the element management tasks even while it is connected to any other management system OS.

#### Stand-Alone Mode

In the stand-alone mode the AEM-NB performs the whole management of the NEs on its own. The user is able to perform all management tasks via the GUI.

Figure 1-1 shows the system architecture in the stand-alone mode.



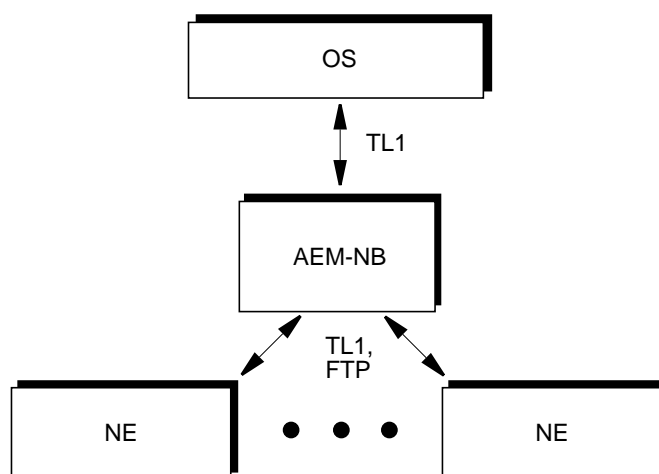
**Figure 1-1 Stand-Alone Mode**

#### Integrated Management Mode

In the integrated management mode the AEM-NB works as an integral part of the customer's management network, providing higher management systems (OSs) with services to manage NEs in their domains.

The AEM-NB allows other OSs to pass provisioning, testing or fault information to and from the NEs, e.g. a fault management surveillance system can collect fault data using the northbound interface.

Figure 1-2 shows the system architecture of the integrated management mode.



**Figure 1-2 Integrated Management Mode**

The complete system and software architecture of the AEM-NB is described in Chapter 1.3, page 1-7.

## 1.3 System and Software Architecture

### 1.3.1 Functional Groups

The AEM-NB software architecture is built with a number of components that can be grouped in the following distinct functional groups:

1. **NE Management**  
(Equipment Management, Service Management, Alarm Management, Test Management, Performance Management)
2. **General Components**  
(Components for Operation, Administration and Maintenance (OAM); Common Servers)
3. **Software Platform**  
(Software bus, Repository, third party libraries)
4. **Graphical User Interface (GUI)**
5. **Northbound Interface**
6. **Southbound Interface.**

Figure 1-3 shows the six functional groups. The shadowed blocks are part of the AEM-NB.

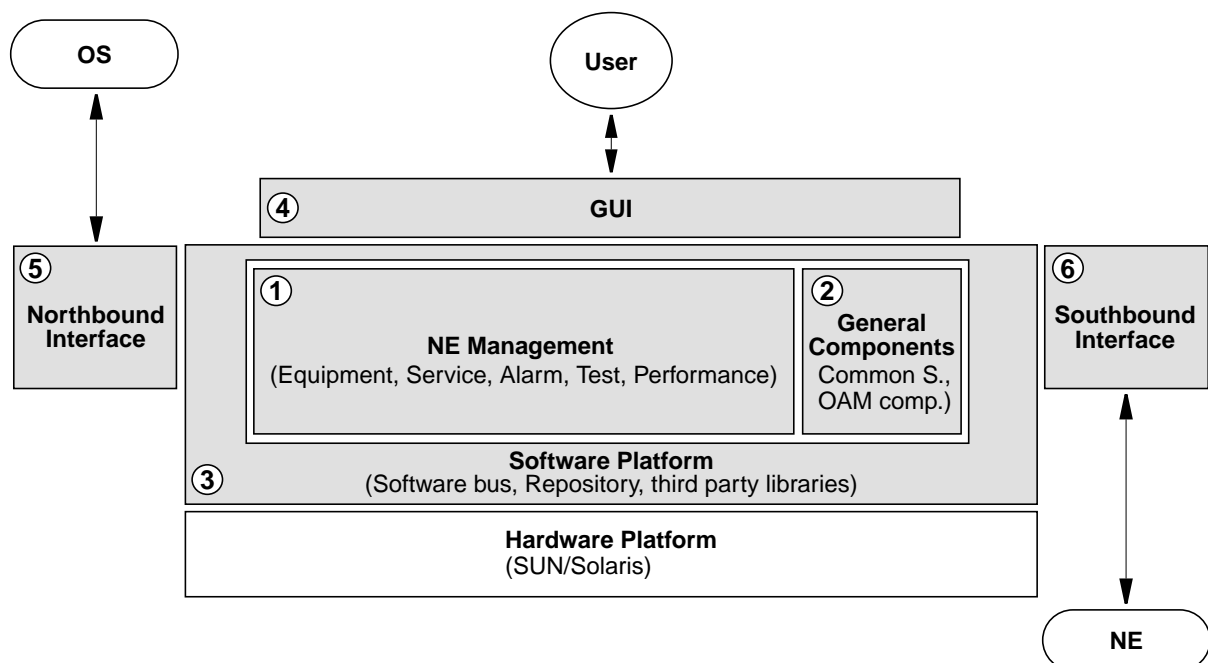


Figure 1-3 AEM-NB Functional Groups

### 1.3.1.1 NE Management

The NE management functionality is distributed in 5 areas. These are: Equipment Management, Service Management, Alarm Management, Performance Management and Test Management.

#### Equipment Management

The Equipment Management provides the following functionality/features:

- *Scrolling List of NEs*

The NEs are displayed in a list covered in a single window called *Network Browser*, where the NEs and their components can be handled like files in a file browser.

- *NE Provisioning*

The operator can create a new NE manageable for the AEM-NB view. The operator must enter the specific configuration data for the new NE such as IP address, NE Name, NE user-id and password.

- *Software Download to a single NE*

Provides a storage medium for maintaining a copy of the software and a mechanism for downloading that software to a NE.

- *Software Download to multiple NEs*

Download of new software to multiple NEs on an individual connection basis.

- *NE Non-Volatile Data Storage Restoration*

Restores NE non-volatile data storage upon user request. Provides a storage medium for maintaining a copy of the NVDS for backup and restore purposes on a periodic basis.

- *Maintain a local Copy of NE Inventory*

The AEM-NB maintains a local copy of specific hardware identifiers and software version identifiers. This local copy accepts automatic inventory notifications. This information can be used for display and report functions in case of loss of communication with the supported NE. The hardware identifiers include all plug-ins.

- *Maintain a local Copy of NE Provisioning Configuration Data*

The AEM-NB maintains a local copy of all cross-connection and parameter settings for each NE. This information can be used for display and report functions in case of loss of communication with the supported NE.

- *Maintain NE Software Copies*

The system keeps a copy of the versions of the NE software running in the NEs (30-channel) managed by the AEM-NB. Generally, only one version of NE software per NE type is used by all the NEs in a network but the AEM-NB must have the capacity to manage two software versions during the upgrade period.



- *NE Reset (INIT-SYS)*

Allows the user to delete the NE and restore the factory settings for the whole NVDS except for the IP address and the target identifier, so that the AEM-NB can still communicate with the NE after the command execution has been completed.

- *AEM-NB Database Synchronization*

Automatic update of the AEM-NB database records based on NE database changes.

- *Protection Control*

The management system provides a facility to allow the user to switch operation of one unit in a NE to a standby unit, if that unit exists.

- *Equipment Protection*

The AEM-NB allows the user to provision the equipment information for the protection scheme. Also the user can force protection switching.

- NE R1.3 COMDAC - simplex/duplex
- NE R1.3 IO\_HDLC - simplex/duplex.

- *NE Timing Synchronization*

The AEM-NB supports the user to configure the NE synchronization clock sources.

- *NE Date and Time*

The AEM-NB allows the user to set and retrieve the date and time of the NE.

- *NE Disaster Recovery from the AEM-NB*

The AEM-NB is able to reconstruct its NE database by polling the NEs for information and from internally maintained backup copies of data.

- *Fiber Reach Support*

The AEM-NB supports the fiber reach by providing alarm information.

- *Support of NE Standby Configuration*

The AEM-NB supports the NE Standby Configuration via the cut-through interface.

**Service  
Management**

The Service Management provides the following functionality/features:

- *NE Service Status*

Provides the aliveness status of the individual NEs providing a customer's service across all NEs under the AEM-NB's control.

- *V5.1/V5.2 Interfaces*
- *Primary/Secondary Links*
- *V5 ISDN User Ports*
- *V5 PSTN User Ports*
- *ISDN Signalling Configuration*
- *V5.2 Protection Group 2.*

- *Network Interfaces and Subscriber Service Provisioning and Activation*

The AEM-NB supports all provisioning functions related to 2-Mbit/s network interfaces and subscriber services. Provisioning contains the creation, deletion and parameter setting/modification of the different subscriber services. The AEM-NB service activation enables and disables the service.

2-Mbit/s network services:

- V5.1
- V5.2
- non-switched services (via cut-through).

Subscriber services:

- analogue telephone (POST) based on V5
- ISDN (2B+D) based on V5
- analogue leased line
- digital leased line (via cut-through).

**Alarm  
Management**

The Alarm Management provides the following functionality/features:

- *Integrated display of all the alarms*

The AEM-NB provides a common window (alarm viewer) to show all alarms reported by the managed NEs or generated by the management system itself. The display shows all the information pertaining to the alarm, including alarm type, severity, service affecting indication, date/time of occurrence and clearing.

- *Alarm Display Filters*

It is possible to filter the items shown in the alarm viewer, for instance, to see only the critical alarms.

- *Alarm Notification to User*

The user is informed by visual and audible alerts when a new alarm has been reported to the AEM-NB.

- *Clearing of Alarms*

Alarms in the management system will automatically be cleared when the faults are removed at the source (such as in the NEs or in the platform). The alarm information will contain the date and time of alarm clearance.

- *Acknowledged Alarms*

The operator can acknowledge a raised alarm - alarm still active but being investigated. The AEM-NB registers the time at which an alarm changes its status from raised to acknowledged and, separately, from acknowledged to cleared. It is also possible for an alarm to go directly from the raised to the cleared state.

- *Alarm Colors*

The management system provides a color scheme based on alarm severities.

- *Enable/Disable of autonomous Alarms on an NE Basis*

- *Fault Localization*

Provides fault localization across all NEs under the AEM-NB control. The COMDAC LEDs show the highest severity alarm for the system. The individual plug-in unit LEDs show the highest severity alarm for the plug-in unit. Fault localization is performed at AP level.

- *NE Alarm Log Handling*

The AEM-NB is able to retrieve the NE alarm log via the cut-through interface.

## Performance Management

The Performance Management provides the following functionality/features:

- *Handling of Performance Records*

Records can be displayed, printed and stored in a user-defined file.

## Test Management

The Test Management provides the following functionality/features:

- *Port Test*

It is possible to request a test for a particular port on a specific application pack.

- *TAP Test*

It is possible to check the correct cabling between the communication interface unit and the test application pack.

- *Standby Card Test Scheduling (via cut-through)*

It is possible to schedule a test to perform a COMDAC side switch or off-line diagnostic for the standby COMDAC or the protection.

- *Built-in Self-Test*

Each NE performs a built-in self-test of plug-ins periodically.

- *Loopback Test at the feeder side*

It is possible to set or clear a loopback on particular feeders.

- *Support of the ISDN Line testing*

Requests a subscriber line testing on a specific list of services (e.g. POTS, ISDN, etc.). The subscriber line tests may consist of the following tests:

- foreign voltage measurement
- insulation measurement
- capacity measurement
- dial tone
- short circuit.

- *Support of CRC test for ISDN drops*

- *Support of Loopback test at the drop side.*

### 1.3.1.2 General Components

The components of this group do not have or require any knowledge of the NEs the AEM-NB is managing. They provide a platform on which the other AEM-NB components can operate and isolate them from the underlying customer platform.

#### OAM Components

The OAM components provide operation, administration, maintenance and security functionality. This is based on third party-tools (i.e. orbix) and a set of specific applications.

The OAM components provide the following functionality/features:

1. **Operation/Administration/Maintenance**

- *Standard Reports*

The system allows the user to generate a set of predefined reports from the information kept by the AEM-NB. The reports cover the following areas:

- Alarms
- Equipment configuration
- Service provisioning
- NE inventory
- Performance.

The reports are available for displaying, printing and saving in a postscript file.

- *Backup and Restore of system relevant data*

Relevant data includes all information necessary to restore the situation in case of an AEM-NB crash.

- *AEM-NB Software Upgrades*

Provides an established release cycle for AEM-NB software upgrades in a way that minimizes incompatibility with NE software releases, and allows for upgrades to provide for OS compatibility. This upgrade does not affect the services provided by NEs.

- *Log Administration*

The logs are capable of being printed and visualized. The system limits the size of the system logs. It is possible to make backups of the logs and to remove them from the system. There are logs for:

- Actions

Contains all the information on actions performed by users or the AEM-NB and which imply changes in the AEM-NB configuration, equipment (NE) configuration, service and subscriber configuration, access to the AEM-NB, print reports and backup & restore, i.e. all operations triggered by the user or the AEM-NB and all subsequent actions. The results of operations are also logged in the actions log.

- System Internal Events

Contains all internal events or actions which report unusual changes in the configuration and state of the AEM-NB or indicate errors that occurred in the AEM-NB.

- Autonomous Reports

Contains all information useful for the equipment supplier about alarms (NE and platform), the performance and all TL1 messages sent from all managed NEs and which imply changes in the database.

- *Possibility to sort logs*

It is possible to show items in the logs while visualizing, saving or printing.

## 2. **Security**

- *Possibility of creating/deleting/modifying AEM-NB Users*

The AEM-NB uses the security mechanisms provided by the SOLARIS Operating System.

- *AEM-NB Security Privilege Levels*

Allows at least three privilege levels within the managed domain. This is mapped to the NE privilege levels accordingly.

- Administrator: has all the permissions.

- Maintenance: has configuration and monitoring permissions.

- Monitoring: has alarm monitoring and testing permissions.

- *NE User Security Privilege Levels*

It is possible to administer the NE users and the privilege levels via the cut-through interface.

- *User Access is authenticated through User Name and Password*

- *Single Login to Access the Domain*

Enables an authorized user to access multiple NEs simultaneously (e.g. multiple windows) using a single login and password.

- *Domain Partitioning*

Enables the NEs managed by the AEM-NB to be partitioned into separate security domains and permits users access to the domains based on their areas of responsibility and profile.

- *User Inactivity Timer*<sup>1</sup>

The user terminal will be locked with a screen saver once a configurable inactivity timer has expired. To unlock the terminal, the user has to type his/her password. The timer has to be configured by the administrator.

- *Lock Screen*<sup>1</sup>

The user is able to lock the screen whenever he wants. To unlock the terminal the user has to enter his/her password.

### Common Servers

Common Servers offer general purpose services. A common server

- manages the AEM-NB history and security logs
- logs the history and security data of other processes upon request
- provides log information upon request
- provides a facility to generate and print client reports in the AEM-NB printers
- provides event distribution services based on a supplier/consumer model.

### 1.3.1.3 Software Platform

#### 1.3.1.3.1 Software Bus

### CORBA Architecture

The communication between the AEM-NB processes is based on the Common Object Request Broker Architecture (CORBA) standard. The heart of the CORBA architecture is the Object Request Broker (ORB). The ORB is a software bus to which different applications can connect to offer their services and/or to use other applications' services (from which they are clients).

The ORB provides a transport mechanism that makes connected servers' location, platform and implementation transparent to their clients, making applications easier to distribute and scale.

### Protocol

The protocol used by the ORB is the Internet Interoperability Protocol (IIOP).

#### 1.3.1.3.2 Repository

### Introduction

The Repository contains all the AEM-NB information that must be persistent. It is supported by an Object Oriented Database (ObjectStore) and the underlying operating file system. All components of the system have direct access to the repository to store/retrieve their own data.

### Contained Information

Information in the repository includes:

1

provided by the SUN Solaris operation system

- NE inventory  
(for each NE: the hardware identifiers and the software versions)
- Equipment and Service provisioning data
- History and security logs
- External system communication parameters
- AEM-NB configuration data
- Alarms cache.

### 1.3.1.4 Graphical User Interface (GUI)

#### Introduction

The Java based GUI is responsible for putting up forms, collecting user input (commands and data) and routing it on to the correct component. It also receives data from the relevant process which it uses to update its display. The GUI has direct access to the services provided by the AEM-NB through the ORB.

#### Functionality, Features

The GUI provides the following functionality/features:

- *Support TL1 messages*  
Supports all TL1 messages for all NE products for dumb terminal access. Allows direct input of TL1 messages. In some markets, direct input of TL1 messages may not be allowed and can be suppressed via the appropriate security permissions.
- *Online Help*  
Provides access to online help which contains at least information on the operation of the AEM-NB, meaning of the buttons, etc.
- *Multiple windowing*  
Provides multiple windowing for access to multiple NE information on a single screen.
- *Multiple user access*  
Provides for multiple users access to the AEM-NB at the same time. Multiple users may include multiple OSs or NMSs as well as multiple GUI access.
- *Time and Date format*  
Enables the user to use local/preferred time and date format. For example, the local calendar must be supported or optional use of 24 hour clock versus a 12 hour clock.
- *User friendly GUIs*  
Provides a user-friendly interface and hides the complexities of the information models.
- *Manageable Objects organized in a Hierarchy*  
The configuration is implemented within a GUI hierarchy:
  - NE group level, containing a number of NEs

— NE level, starting with shelf-view.

- *GUI process to be separated*

The graphical interface driver can be placed on a separate platform from the rest of the EMS application.

### 1.3.1.5 Northbound Interface

**Tasks** The Northbound Interface performs all the tasks needed to communicate to other OSs. It allows external OSs access to the NEs managed by the AEM-NB directly through TL1 commands via a Northbound Interface. This access is controlled by the Northbound Interface until the OS is disconnected.

**TL1 Northbound Interface** The TL1 Northbound Interface allows an external OS access to the NEs managed by the AEM-NB directly through TL1 commands for provisioning, testing and alarm purposes.

### 1.3.1.6 Southbound Interface

**Tasks** The Southbound Interface performs all the tasks needed to communicate to the NEs managed by the AEM-NB. It provides distributed CORBA access which includes implementation and translation of TL1 commands, response and autonomous messages into equivalent CORBA requests and events.

**TL1 Southbound Adaptors** The TL1 Southbound Adaptors isolate the main AEM-NB functionality from the specific protocols used by the NEs. They are responsible for translating actions and state changes conveyed through CORBA messages from/into the NE specific message formats.

**Functionality, Features** The Southbound Interface provides the following functionality/features:

- *Southbound TCP/IP TL1 Client Application*  
Support for the TL1 client application on the southbound TCP/IP interfaces. TL1 is used for most of the OAM&P functions (see Chapter 1.3.1.2, page 1-12).
- *Southbound TCP/IP FTP Client Applications*  
Support for the FTP client application on the southbound TCP/IP interfaces. FTP is required for software download and NE data backup/restore.
- *Southbound TCP/IP Telnet Client Applications (Cut-Through)*  
Support for the Telnet application on the southbound TCP/IP interfaces. Telnet is used to provide a direct command line into the NE (i.e. an equivalent ASCII terminal interface).



## 1.3.2 Hardware Platform

### 1.3.2.1 Architecture

#### Components

A number of AEM-NB Clients (UNIX Workstations) can be added to the AEM-NB Server to support concurrent users or remote access to the server's applications. These clients can be connected through a TCP/IP infrastructure or a Local Area Network (LAN). Examples are shown in Figure 1-9, page 1-28 to Figure 1-12, page 1-31.

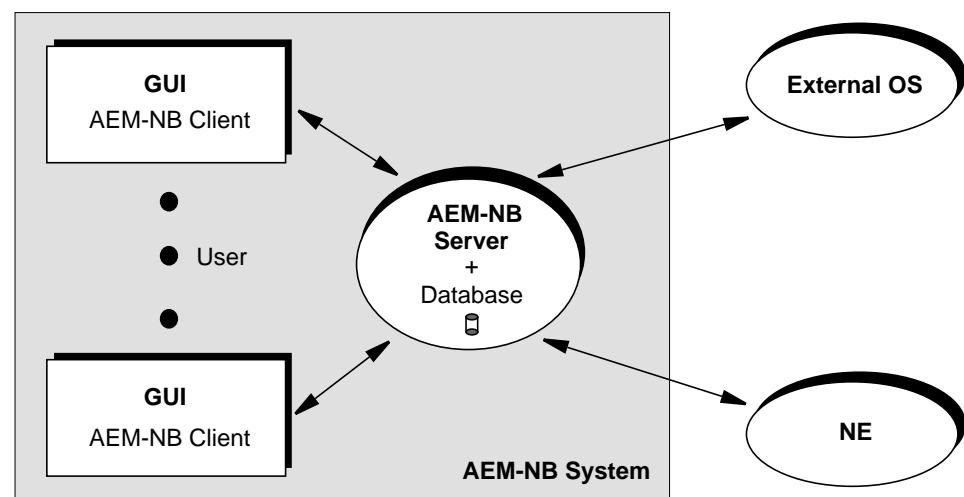
#### Tasks of the Components

The tasks of the components are:

- **AEM-NB Server:**  
Manages all the AEM-NB applications and provides access to the NEs, the database and the external OS.
- **AEM-NB Client:**  
Formats the display of the application screens and manages the users sessions with the application, e.g. database access.

#### Conceptual Representation

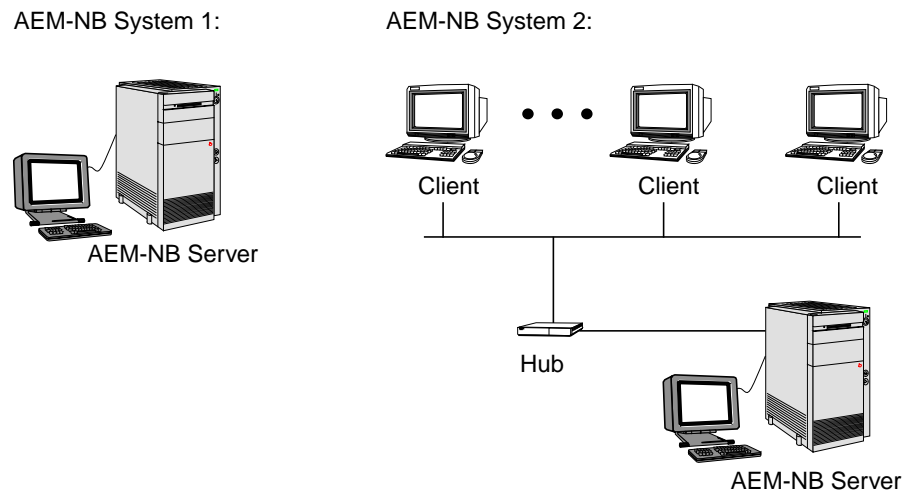
Figure 1-4 is a conceptual representation of the various generic components.



**Figure 1-4 Hardware Components**

## Examples of AEM-NBs

Two examples of an AEM-NB system are shown in Figure 1-5.



**Figure 1-5 Examples of AEM-NBs**

### 1.3.2.2 Requirements

#### Server/Clients

A SUN SOLARIS workstation can be used as AEM-NB Server as well as AEM-NB Client.

#### Peripherals

The AEM-NB system may use a number of peripherals with the following tasks:

- **CD-ROM:**  
Used for installing the system software.
- **Tape drive or another removable device (optional):**  
Used for backup and restore functions.
- **Printer:**  
Used for obtaining hard copies, e.g. configuration/alarm reports or performance monitoring measurement information.

## 1.4 Working with AEM-NB

### Goal of this Chapter

This chapter will outline the management activities and processes in the AEM-NB. The main emphasis is on presenting everyday operation processes. The chapter is structured with respect to the various network life cycle phases (see further below).

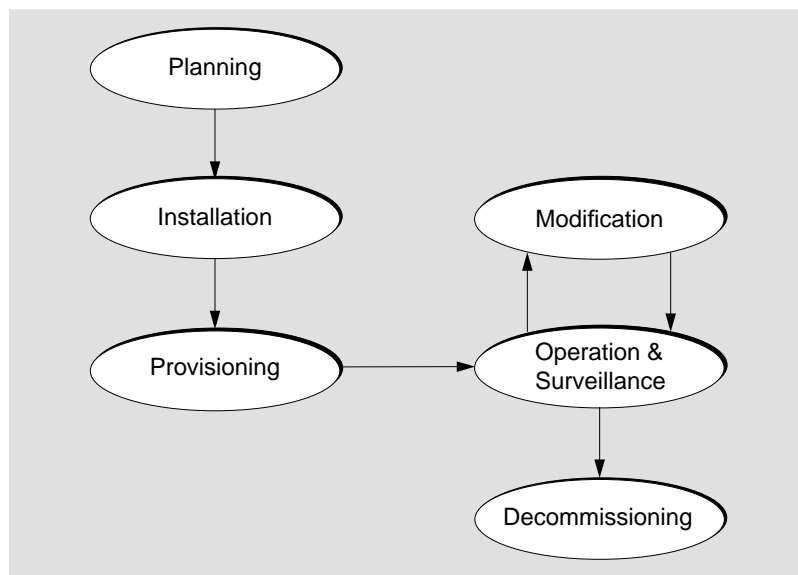
### User Profiles

There are 3 default user profiles: the administrator, maintenance and monitoring profile. The rights belonging to these profiles are described in Chapter 1.4.4, page 1-27.

### Life Cycle of a Network

The individual life cycle of a telecommunication network has the following phases: planning, installation, provisioning, operation & surveillance, modification and finally decommissioning. Modification of a network may take the form of fine adjustment, expansion or restructuring of the network, and addition of new functionality.

Figure 1-6 shows the life cycle of a network.



**Figure 1-6 Life Cycle of a Network**

### Support by AEM-NB

The AEM-NB is mainly used in three life cycle phases: during network provisioning, network modification and network operation & surveillance. The installation phase is supported by the Graphical System Interface for Narrowband Services (GSI-NB).

### 1.4.1 Network Planning and Physical Installation

---

<b>Network Planning</b>	In the network planning phase, all specifications and requirements of the future network operation are translated into a concrete network structure. That means, the network planning phase, during which a decision on the network topology, equipment and components is made, has to take place before the operation with the AEM-NB starts.
<b>Physical Installation</b>	<p>The installation of the network follows the planning phase. The installation includes the following steps:</p> <ul style="list-style-type: none"><li>■ Physical NE installation. This includes the installation of racks, plug-ins and cabling of the NEs.</li><li>■ Creation of a DCN plan Communication between the AEM-NB and the NEs is carried out via the Data Communication Network (DCN). A DCN plan should be drawn up before provisioning the network to ensure that the AEM-NB can reach all NEs and that the administration of the DCN does not lead to an undue increase in performance requirements.</li><li>■ NE connection to the AEM-NB server</li><li>■ OS connection to the AEM-NB Server (optional)</li><li>■ Installation of the third-party, application and AEM-NB software on the AEM-NB Server.</li></ul>
<b>Network Status after Physical Installation</b>	After completion of these steps, the network operator has at his disposal a network which is connected physically with AEM-NB and which is, in principle, ready for operation.

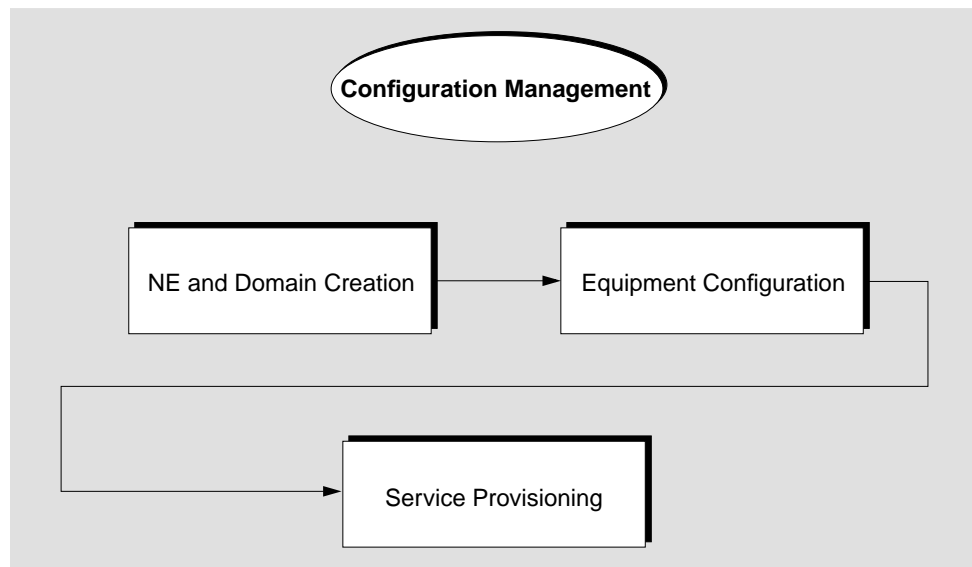
## 1.4.2 Configuration Management

### Introduction

The Configuration Management in accordance with the specific operating conditions of the network operator is performed by special provisioning actions. It is assumed that the NEs and AEM-NB have already been physically connected.

### Provisioning Actions

Figure 1-7 provides an overview of the provisioning actions and the text which follows gives a detailed description.



**Figure 1-7 Network Provisioning**

### NE and Domain Creation

Prior to equipment configuration and service provisioning, the NEs must be known in the AEM-NB. To achieve this, the following 4 steps are necessary:

1. Creation of domains
2. Creation of NEs
3. Assignment of NEs to any domain(s)
4. Logical connection of NEs.

All steps are described in detail in Chapter 5.

### Equipment Configuration

NEs can be configured if they are known in the AEM-NB. The following measures should be performed:

- Selection of the timing synchronization source
- Selection of the COMDAC (simplex/duplex) and IO\_HDLC protection scheme
- Selection of those slots for which an absence of the plug-in will be alarmed (only applicable for COMDAC)

- Provisioning of card types which are inserted in a slot
- Configure ISDN in POTS mode via cut-through
- Provisioning of the protection switching.

All steps are described in detail in Chapter 5.

#### **Service Provisioning**

If the NEs are configured and integrated in the network, cross connections can be defined. The following actions are necessary:

- Creation of V5 Network Interfaces
- Adding of V5 Links to the V5 interfaces
- Adding of Primary/Secondary Links
- Adding of V5 User Ports.

All steps are described in detail in Chapter 5.

#### **Network Status after Provisioning**

After the provisioning phase the NEs can now be controlled and monitored by the AEM-NB and start operation & surveillance.

### **1.4.3 Network Operation & Surveillance**

#### **Actions**

During network operation & surveillance, the administration, control and supervision of the network mainly include

- Fault Management
- Network Modification
- Performance Monitoring.

#### **Required Rights**

The administrator rights are sufficient to perform all required operations. The visual check of parameters and displays on the GUI requires monitoring rights only.

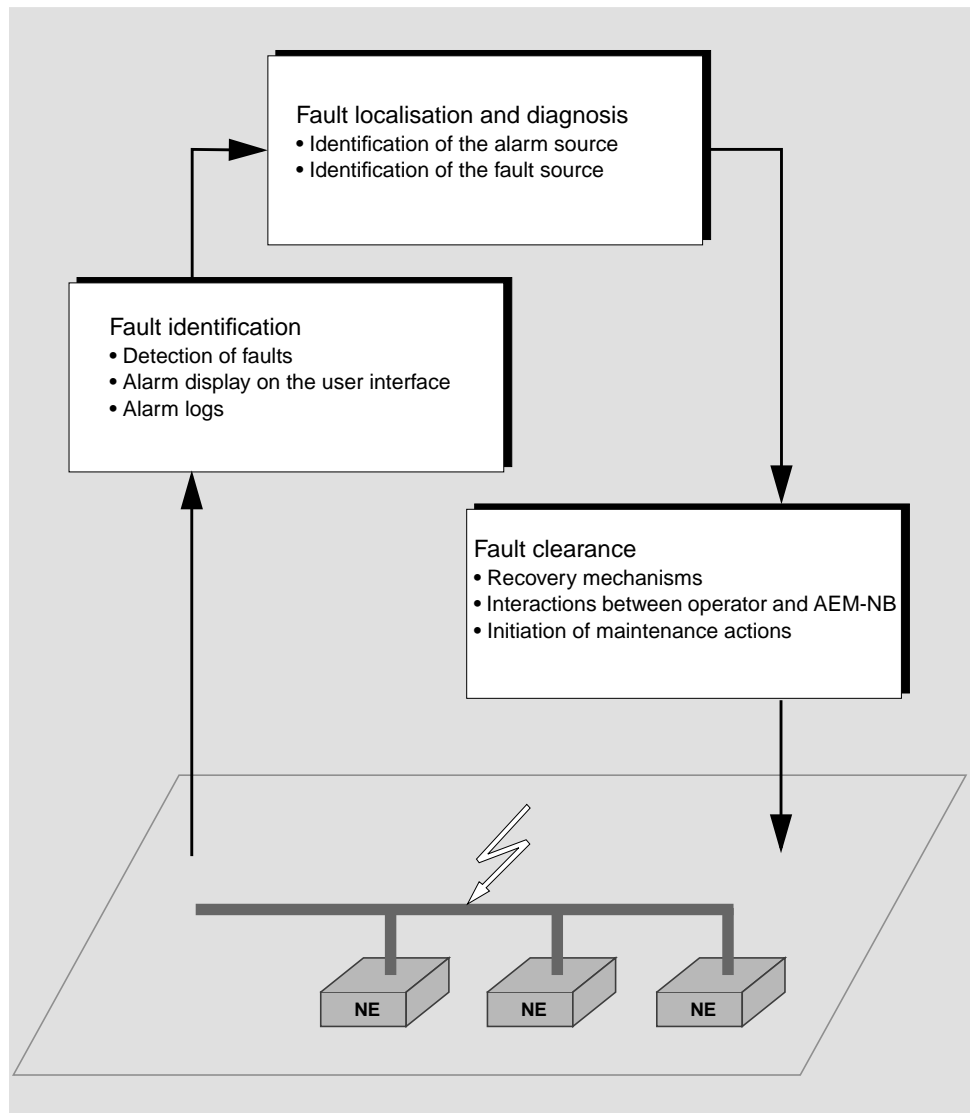
#### **1.4.3.1 Fault Management**

##### **Alarm Types**

There are two alarm types: alarms generated by the NEs and alarms generated by AEM-NB itself, e.g. an alarm indicating that log files without archiving is being removed (LOG\_DEL\_FULL). All alarms are displayed in the alarm viewer. It allows the network operator to detect the alarm and to locate its source.

##### **General Fault Handling**

Figure 1-8 shows the general fault handling. In the following the individual phases are described in more detail.



**Figure 1-8 General Fault Handling**

#### 1.4.3.1.1 Fault Identification

##### Background

AEM-NB gathers information about faults occurring in the network and forwards this information to the network operator. This procedure includes two tasks: on the one hand, the fault must be identified, and on the other hand, the fault information must be processed as alarm notifications to be displayed on the user interface.

##### Detection of Faults

If an NE fault is detected, the NE notifies the AEM-NB. The notification comprises the type of fault and the address of the originating NE. The AEM-NB detects and processes such a notification automatically.

If the unit of a NE fails that is responsible for the communication with the AEM-NB, the fault is identified differently. No alarm notification will be sent to the AEM-NB. The AEM-NB detects the fault by testing at regular intervals whether the association to the particular NE is dropped. In this case the AEM-NB itself raises an alarm.

#### **Alarm Display on the User Interface**

A complete alarm overview and a detailed alarm description is provided by the alarm viewer. All relevant alarm data (e.g. alarm severity) are shown.

#### **Alarm Logs**

The AEM-NB keeps alarm logs to store the alarm notifications. Alarm logs are used among other things for long-term observations, e.g. of the fault behaviour in the network. Alarm logs exist for pending alarms, for the alarm history and for clock events in the network.

### **1.4.3.1.2 Fault Localisation and Diagnosis**

#### **Reaction to Fault Identification**

When a fault has been detected, it is necessary to localise its source and diagnose its cause in order to initiate appropriate repair procedures. To locate the cause of fault, the AEM-NB provides information gathered from alarm notifications and general network data.

#### **Fault Source**

Each alarm notification contains the name of the network component from which it originates. This network component, however, need not always be the real fault source.

### **1.4.3.1.3 Fault Clearance**

#### **Background**

The AEM-NB detects faults automatically and clears various software errors by itself (fault recovery). The transmission characteristics of the network will not be impaired by this.

#### **Recovery Mechanisms**

System Recovery protects the AEM-NB and associated users from unnecessary problems and avoids or reduces manual work.

Recovery processes vary depending on the type of failure that occurred, the structures affected, and the type of recovery. If no files are lost or damaged, recovery may amount to no more than restarting an instance. If data has been lost, recovery requires additional steps, such as database restore using a previous backup.

AEM-NB recovery mechanisms are initiated mainly by the following situations:

- NE software crash
- AEM-NB crash
- Communication between AEM-NB and a NE is interrupted.

In the case of a NE crash, the AEM-NB configures NEs in accordance with the internal state of the AEM-NB database. In the event of a AEM-NB crash or an interruption in communication, the AEM-NB downloads the current NE configuration from the NE to its database.



**Interactions  
between Operator  
and AEM-NB**

Faults (software or hardware), the cause of which the AEM-NB cannot eliminate itself by means of a recovery mechanism, must then be handled by the user. The AEM-NB supports this. The AEM-NB first displays the fault on the user interface. The user then initiates appropriate measures to clear the fault and/or to maintain network operation. This includes access to faulty network units and the redirection of the network traffic. The AEM-NB supports both.

**Initiation of Main-  
tenance Actions**

Sometimes, additional maintenance actions are necessary to clear a fault. For example, some network disturbances can also originate in hardware faults. Such hardware faults often require the faulty component to be replaced, and this can only be done by maintenance personnel.

**NOTE:**

More detailed information about maintenance actions is provided in Chapter 6.

**Fault Clearance**

Once the fault has been cleared, the alarm is reset automatically.

**1.4.3.2 Network Modification****Types of Network  
Modification**

Usually, network operation & surveillance requires structural modifications in the network. The AEM-NB supports this. There are two types of network modifications:

- Installation or removal of NEs
- Modification of NEs.

**1.4.3.2.1 Installation and Removal of an NE****Installation of a NE**

For installing a new NE in an existing network the following steps must be carried out:

1. Check whether the new NE can be incorporated in the existing DCN plan drawn up in the network planning phase (if not, the DCN plan must first be revised)
2. Creation of the NE
3. Assignment of the NE to a domain
4. Logical connection of the NE
5. Selection of the timing synchronization source
6. Selection of the COMDAC protection scheme (simplex/duplex)
7. Selection of those slots for which an absence of the plug-in will be alarmed (COMDAC)
8. Provisioning of card types which are inserted in a slot.

All steps are described in detail in Chapter 5.

**Removal of an NE** If an NE is no longer managed by the AEM-NB, the administrator deletes it from the AEM-NB database.



**NOTE:**

When an NE is deleted from the AEM-NB database, it is still fully functional. The TL1 and TCP/IP links between the AEM-NB and the NE will be closed and the management access via the AEM-NB is not possible until the NE is created and connected again.

#### **1.4.3.2.2 Modification of NEs**

**Adding a Plug-in** NEs can be modified by adding or removing plug-in units. The AEM-NB recognises automatically which plug-in unit has been plugged and where. As only default settings are set on the new plug-in unit, the system administrator must adapt the configuration.

**Removing a Plug-in** When deleting a plug-in, it must be ensured that there are no connections running via this unit. Then the plug-in may be removed.

#### **1.4.3.3 Performance Monitoring**

**Tasks of Performance Monitoring** Performance management guarantees that the transmission quality does not fall below a minimum performance threshold.

Another task is the recording of data for analysis at a later date, e.g. storing alarms in logs and print them.

#### 1.4.4 System Security and User Groups

##### Protection from Unauthorised Access

The AEM-NB provides mechanisms which protect the system from unauthorised access. The user groups play a very important role in this context as they define different levels of access rights for the individual users.

##### User Groups

By default there are 3 user groups: the administrator, maintenance and monitoring user group. Further groups can be added.

##### Access Rights

Table 1-1 provides an overview of the access permissions the user groups should have.

**Table 1-1 Assignment of User Groups to Applications/Tasks**

Application	Task	User Group
System Administration	Start-up / Shutdown	Administrator
	Monitoring	Administrator
User Administration and Profiling	Access Policy Management	Administrator
	Domain Management	Administrator
Log Viewer	Actions	Administrator, Maintenance
	System Internal Events	Administrator, Maintenance
	Autonomous Report	Administrator, Maintenance, Monitoring
Alarm Viewer	Acknowledge	Administrator, Maintenance
	View	Administrator, Maintenance, Monitoring
	Clear	Administrator, Maintenance
Configuration Manager	NE Creation	Administrator, Maintenance
	Equipment and Service Provisioning	Administrator, Maintenance
	View	Administrator, Maintenance, Monitoring
	Test	Administrator, Maintenance, Monitoring
	Scripts	Administrator
	Cut-through	Administrator
BroadBand EM	BroadBand EM	Administrator, Maintenance, Monitoring

## 1.5 Network Configuration

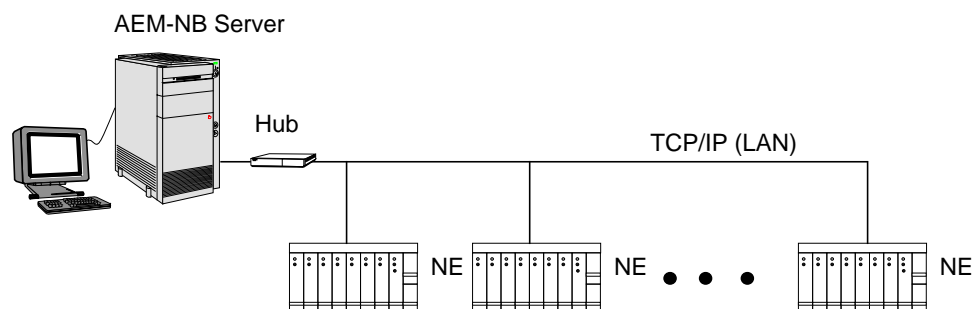
The network configuration depends on the user applications. The most probable configurations are described below and illustrated in Figure 1-9 to Figure 1-12.

**NOTE:**

If there are various configuration options of the DCN, these are shown in the figures by means of dashed lines. The hubs are optional depending on the number of client platforms and NEs.

### 1.5.1 AEM-NB Server without Clients and external OS (LAN)

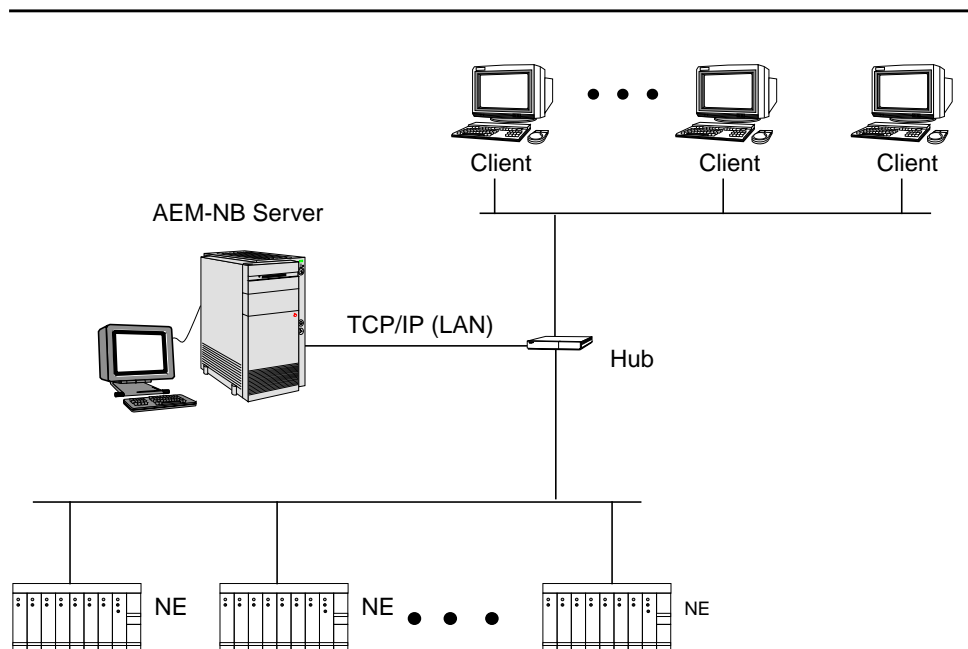
AEM-NB server connected to the NEs using a Local Area Network (LAN).



**Figure 1-9 AEM-NB Server without Clients and external OS (LAN)**

### 1.5.2 AEM-NB Server with Clients and without external OS (LAN)

AEM-NB server and one or more clients connected to the NEs using a LAN.



**Figure 1-10 AEM-NB Server with Clients and without external OS (LAN)**

### 1.5.3 AEM-NB Server without Clients and with external OS (WAN)

AEM-NB server connected to the NEs using a LAN and connected to one or more external OSs using a WAN link.

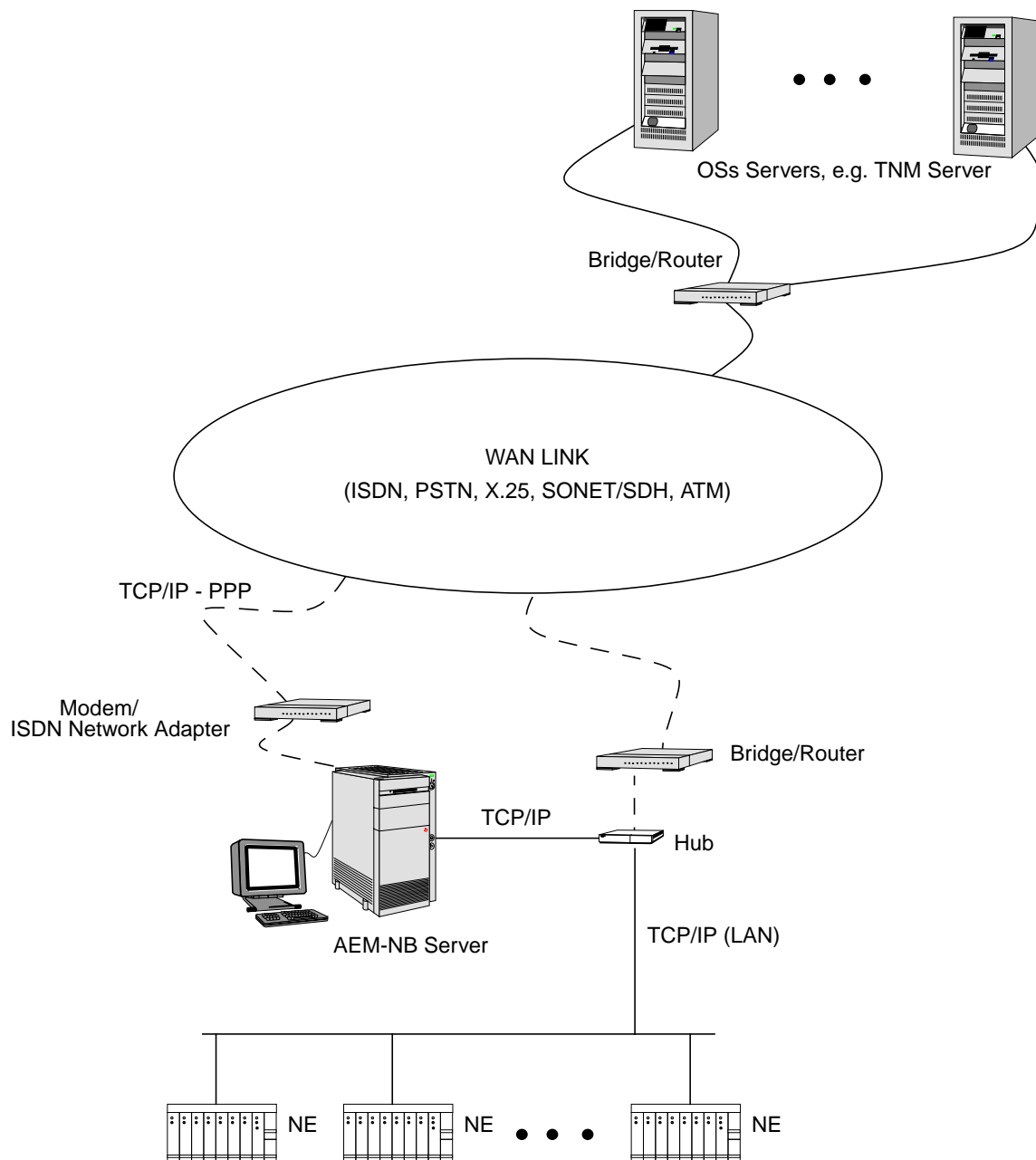
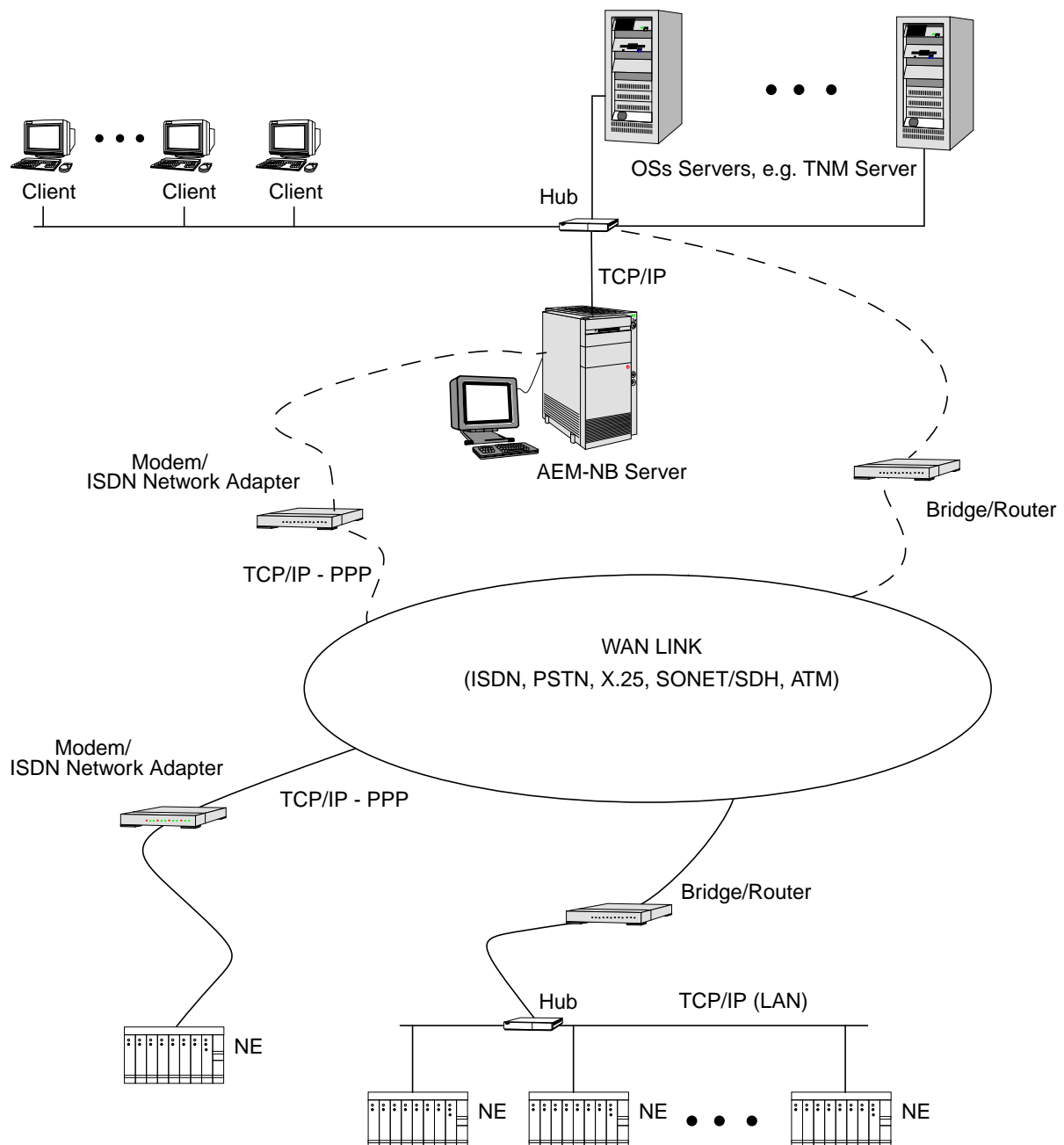


Figure 1-11 AEM-NB Server without Clients and with external OS (WAN)

### 1.5.4 AEM-NB Server with Clients and external OS (WAN)

AEM-NB server and one or more clients connected to the NEs using a WAN link and connected to one or more external OSs using a LAN connection.



**Figure 1-12 AEM-NB Server with Clients and external OS (WAN)**





---

## Contents

<b>2.1</b>	<b>General</b>	<a href="#"><u>2-1</u></a>
2.1.1	Introduction	<a href="#"><u>2-2</u></a>
<b>2.2</b>	<b>Installation Procedure</b>	<a href="#"><u>2-6</u></a>
2.2.1	Full Installation	<a href="#"><u>2-6</u></a>
2.2.1.1	Server Side Installation	<a href="#"><u>2-7</u></a>
2.2.1.2	Client Side Installation	<a href="#"><u>2-27</u></a>
2.2.1.3	Post-Install Actions	<a href="#"><u>2-40</u></a>
2.2.1.3.1	AEM-NB Server	<a href="#"><u>2-40</u></a>
2.2.1.3.2	AEM-NB Client	<a href="#"><u>2-40</u></a>
2.2.2	Installing Individual Packages	<a href="#"><u>2-40</u></a>
2.2.3	Cancel Installation	<a href="#"><u>2-43</u></a>
2.2.4	Remove <i>AnyMedia</i> Package Installations	<a href="#"><u>2-43</u></a>
2.2.4.1	Remove <i>AnyMedia</i> Servers Package	<a href="#"><u>2-43</u></a>
2.2.4.2	Remove <i>AnyMedia</i> Client Package	<a href="#"><u>2-44</u></a>
2.2.4.3	Remove Third-Party Packages	<a href="#"><u>2-46</u></a>

---

## Contents

---

## 2.1 General

The AEM-NB R1.3 (*AnyMedia*® Access System Element Manager for Narrow-band Services, Release 1.3) runs on SUN SPARC Solaris 2 computers running Solaris 2.5.1 plus security and Y2000 patches and patch 106255-01 recommended by SUN.

In order to successfully install the AEM-NB R1.3 for the SUN Solaris installation the following has to be taken into account:

- **Disk partitioning:**  
HDD partitioning should include, in addition to the standard UNIX entries (e.g. /, /usr, /var, etc.), two entries for the AEM-NB software and the transaction.log (cf. Chapter 2.1.1, page 2-2 for size requirements).
- **Swap space:**  
In addition to the SUN recommendation (at least double the size of the RAM memory should be used for swap), 100MB per platform should be configured for OODBMS requirements.
- **NIS:**  
If more than one AEM-NB platform is to be used, NIS should be configured in the server, so all the AEM-NB clients will share the logins and password which are configured in the server tables. All the users require a NOT null password in order to manage AEM-NB.
- **NFS:**  
Network File Sharing is not required even when using a LAN, but if NIS is used, NFS allows operators to log-in in any client platform having access to their home directories.
- **SUN patches:**  
All the Solaris patches described in the shopping list must be installed before AEM-NB installation

- **LAN & WAN configuration:**  
E.g. default router to NEs, etc. must be available.

How to install SUN Solaris is described in SUN support/SUN Solaris Installation Guide.

### Assumptions

For the following description it is assumed that

- the hardware required to install the AEM-NB R1.3 is prepared
- the AEM-NB R1.3 consists of a number of server and client applications. The software installation may imply the installation of all these applications or only some of them.

### JRE

- the AEM-NB R1.3 includes as part of its environment the Java Runtime Environment (JRE) Release 1.1.7. JRE is included here free of charge for the final user.

## 2.1.1 Introduction

### System Requirements

This document is intended as a guide for the person(s) who will be responsible for the installation and configuration of the hardware and software required for the AEM-NB R1.3 installation.

The *AnyMedia* distribution can be divided into two parts, server-side installation and client-side installation. Both include specific third-party applications needed to run the *AnyMedia* successfully.

### Disk Space

To store the AEM-NB R1.3 files, your system must have the following amount of free disk space:

- AEM-NB client: 60 MB
- AEM-NB server: The space will depend upon the number of NEs managed by the system because of the data size. The recommended size for n NEs is obtained from adding the following (numbers in kbyte):

software=450000

logs=15000

databases=1400+600\*n

transactions=2\*(800+350\*n)+n+25%

The size calculated is based on maximum configurations and includes the overhead necessary for the temporary data used in operation.

It is recommended to create a separate partition to locate the transaction log file needed by ObjectStore. This partition would be used for this purpose only. It must not be deleted or managed because this file is only created and managed by ObjectStore. Note that without this file ObjectStore is not able to work and also if a new partition or location is chosen, it needs write permissions for the *AnyMedia* user (login). If you choose a directory under *AnyMedia* location the correct owner and permits will be automatically provided in the installation process of *AnyMedia*.

The following table shows the recommended size of the partitions for a maximum of 10, 40 and 100 NEs:

NEs	/part 1	/part 2
10	475 MB	11 MB
40	500 MB	37 MB
100	530 MB	100 MB

where /part1 contains all the AEM-NB server software and data bases and the /part2 is dedicated to the transaction log.

### Distribution Media

The AEM-NB R 1.3 distribution media is on CD-ROM and the default installation directories are /opt/lucent/*Application\_name* (refer to Table 2-1, page 2-4 for more information about application names).

The AEM-NB R1.3 distribution is divided into twelve packages, as follows:

- *AnyMedia* Servers
- *AnyMedia* Client (GUI)
- *AnyMedia* Help
- Netscape Navigator 4.51
- OrbixMT2.3c patch 02
- OrbixTalk 1.2c patch 02
- OrbixNames1.1c
- OrbixWeb 3.0
- ObjectStore5.0
- jre1.1.7+symantec+ReportPro
- LUMOS build 6
- RogueWave 1.0.7 & 1.1.2.

These were built using the application packaging tools offered by Solaris (refer to your SUN documentation for more information).

A package contains a collection of files and directories required for the application and scripts to control how, where and if the package is installed.

**Table 2-1 AEM-NB R1.3 Distribution Description**

Package Name	Application Name	Description
LuANY15S	<i>AnyMedia</i> Servers	The set of CORBA (Common Object Request Broker Architecture) servers containing the business logic (element management functionality).
LuANY15C	<i>AnyMedia</i> Clients	An easy-to-use, window-based user interface to the element management functionality.
LuANY15en	<i>AnyMedia</i> Help	A browser-based, on-line user manual.
LuLUMRT	Lumos build 6 RT	A server providing distributed access for TL1 and SNMP-managed NEs. Provides CORBA/TL1 translations
LuNETSCP	Netscape Navigator 4.51	Stand alone.
LuOXNSRT	OrbixNames 1.1c RT	A full implementation of the name service as defined by the OMG (Object Management Groups)
LuOX23RT	OrbixMT 2.3c patch02 RT	A full implementation of the OMG CORBA for C++. It provides an efficient paradigm of client-server programming, allowing easy deployment of distributed systems.
LuOSRT	ObjectStore 5.0 RT	An object oriented database management system (OOD-BMS) providing persistent storage for AEM-NB data.
LuOXTKRT	OrbixTalk 1.2c patch 02 RT	A full implementation of the event service as defined by the OMG.

**Table 2-1 AEM-NB R1.3 Distribution Description**

Package Name	Application Name	Description
LuOXWRT	OrbixWeb 3.0 RT	A full implementation of the OMG CORBA for Java.
LuRWRT	RogueWave 1.0.7 & 1.1.2 RT	A set of standard programming libraries used by the AEM-NB servers.
LuJRERT	jre 1.1.7 + symantec + ReportPro	Java platform environment for the graphical user interface.

**NOTE:**

RT describes a Run Time application version.

**Pre-requisites**

The Netscape 4.5 application may have already been installed on the target system (only needed to display Help and to start AEM-BB). In this case it can be skipped during the installation process (see step 71, page 2-35).

**TCP Ports**

The following TCP ports **must** be available in order to successfully run the AEM-NB R1.3:

- 1570: Orbix daemon uses the TCP port 1570 in order to wait for incoming connections that use the Orbix protocol.
- 1591 to 1641: As COBRA servers are activated by the Orbix daemon, they are assigned to a port that clients can communicate with.
- OrbixTalk uses two ports for communications. These ports have as default values "5000" and the next available value. The first value can be modified at installation time to a value between 1024 and 65534. It is essential that these ports are not used by any process on the SAME SUBNET DOMAIN.

**IP Multicast Addresses**

IP multicast addresses:

Using OrbixTalk, all communication take place using multicast addresses. OrbixTalk can use up to 31 IP multicast addresses with 255.0.0.0 as the first IP address (it is configurable at installation time in the range 255.0.0.0 to 239.255.255.255).

**Time Zone**

The time zone **must** be the same for the *AnyMedia* client <GUI>, LUMOS, Network Element and OS. This parameter is needed for installing the *AnyMedia* client.

The install\_AMEMR15 script runs in the korn shell <ksh> environment.

## 2.2 Installation Procedure

### General

The AEM-NB R1.3 distribution includes an installation script called `install_AMEMR15` which shall be used in a full installation (it includes all packages stored on the distribution media). Also, you can make individual package installations using the `pkgadd` command or using the `admintool` (system administration with a graphical interface). In this case, you must be very careful with the packages dependencies showed in "Packages Dependencies" on page 40.

This guide shows the flow of the installation - according to the interaction with the administrator - using the installation script provided in the distribution and using the `pkgadd` command for individual installations.

### Common Tasks

Common actions must be make in both cases, as follows:

- You need to be logged on as `root`.
- Get ready your distribution medium:

### Insert and Mount the CDROM

Insert and mount the CD. If the machine is running the `vold`, it will recognize that the CD is in place and mount it on `/cdrom/AnyMediaNBEMR15` (depending on your system configuration, `/cdrom/AnyMediaNBEMR15` might have to be replaced with a different device name). Depending on the configuration of `vold` you may have to append a trailing dot (".") to references to file names on the CD. This is due to `hsfs` imposing a suffix on the file names. If the machine is not running the `vold`, type:

```
# mount -F hsfs -o ro,notraildot
/dev/dsk/c0t6d0s2/cdrom
```

The device identifier `c0t6d0s2` is configuration dependent, and as such will vary from machine to machine.

This will mount the CD on `/cdrom` (depending on your system configuration, `/cdrom` might have to be replaced with a different mount point. For more information about on how to mount a CD-ROM drive refer to your SUN documentation.

### 2.2.1 Full Installation

This type of installation uses the `install_AMEMR15` script in order to install all packages contained in the distribution.

For the following description it is assumed that:

- The hardware and software requirements to install the AEM-NB R1.3 are prepared
- AEM-NB R1.3 software have not been installed previously.
- Common actions showed above have been made
- A new user shall be created on the target system, who will be the owner of the AEM-NB R1.3 files. The server workstation shall be a NIS server and the client workstations shall be NIS clients. All the users shall be included



in NIS and exported through the network in order to be recognized by the AEM-NB software. For more information about the NIS tools refer to your SUN documentation.

- A NIS group is also necessary. Typically a new group shall be created to include all the AEM-NB users.

### Procedure

Complete the following procedure to install the AEM-NB R1.3 application.



#### NOTE:

Lines with indentation and quoted are the system responses. They are included here to guide the installation procedure.

### 2.2.1.1 Server Side Installation

Complete the following procedure to install the *AnyMedia* server side. After you have installed the server side the machine should be to rebooted.

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Go to the directory where the installation script is placed (cdrom or disk) |
| 2. | Type <code>./install_AMEMR15</code> and press Return.                       |

```
AnyMedia NB EM R1.5 installation
```

```
CopyRight (c) 1999 Lucent Technologies, Inc.
All Rights Reserved
```

```
**Pre-requisites**
```

```
1.- Before attempting to install the applica
tion, please,read the readme.txt file.
```

```
2.- AnyMedia NB EM R1.5 runs on SUN SPARC So
laris 2 computers running Solaris 2.5.1 plus se
curity and Y2000 patches recommended by SUN and
106255-01 patch.
```

```
3.- TCP ports:
```

```
The following ports MUST be available in order
to succesfully run the AnyMedia EM:
```

```
* 1570: Orbix daemon uses the TCP port 1570 in
order to wait for incoming connections that use
the Orbix protocol.
```

```
* 1591 to 1641: As Corba servers are activated
by the Orbix daemon, they are assigned a port so
that clients can communicate with it.
```

```
* OrbixTalk uses two ports for communications.
These ports have as default values "5000" and
the next one. The first can be modified
```

at installation time to a value between 1024 and 65534. It is essential that these ports are not used by any process on the SAME SUBNET DOMAIN.

4.- IP multicast addresses:

Using OrbixTalk, all communications takes place using multicast addresses. The range of IP multicast addresses used by OrbixTalk is 31 with 255.0.0.0 as the first IP address (it is configurable at installation time in the range 255.0.0.0 to 239.255.255.255)

5.- The install\_AMEMR15 script runs on K-shell <ksh> environment.

6.- The time zone MUST be the same for the Any Media Client <GUI>, LUMOS and Network Element. This parameter is needed for installing the Any Media Client.

\*\*\*\*\*

Do you like to continue [y,n,?,q]

3. Type **y** and press **Return** to continue or type **n** or **q** and press **Return** to exit.

"AnyMedia NB EM R1.5 installation"

"CopyRight (c) 1999 Lucent Technologies, Inc."

"All Rights Reserved."

"Please, choose the installation mode"

" 1 Client <Client side installation>"

" 2 Server <Server side installation>"

"Enter selection [?,?,q]:"



**NOTE:**

Type **?** to get help, type **??** to repeat the prompt and type **q** to exit from the installation.

4. Type **2** and press **Return**

**LUMOS Build 6 Installation**

```
"Packages to be installed: LuLUMRT, LuRWRT,
LuOX23RT, LuOXNS, LuOXTKRT, LuOSRT"
```

```
"Processing package instance <LuLUMRT> from
<XXXXXXX>"
```

**NOTE:**

xxxxxxx shows the path where the package is installed.

```
"Lumos Runtime for AnyMedia NB-EM R1.5"
```

```
"(sparc-solaris) Build 6 run-time"
```

```
"OK, No previous package LuLUMRT have been
found."
```

```
"Enter install directory [/opt/lucent/LUMOS]
[?,q]"
```

5. Type a valid path where the package files must be placed and press **Return** (press **Return** to select default).

If the DNS domain is found:

```
"The DNS domain name found was: xxxxxxxx"
```

```
"What is your DNS domain name [default: xxxxxxxx]"
```

If the DNS domain name is not found:

```
"The DNS domain name has NOT been found."
```

```
"Maybe this machine does not have DNS or is not
configured."
```

```
"If you do not have DNS then press RETURN to the
next question."
```

```
"In other case write your DNS domain name
selection or accept the default."
```

```
"What is your DNS domain name [default: ]"
```

6. Type your DNS domain name and press **Return** (press **Return** to select default - available only if DNS domain was found).

**NOTE:**

A list of DNS user:group items of the target system is displayed (for instance, anymedia:lucent). This provides information to select an user owner and a group owner for packages files.

```
"Select owner and group for package files."
"NBR  USER:GROUP"
"  1  anymedia:lucent      "
"  ....  "
"Enter selection [?,??,q]:"
```

7. Type an user:group number and press Return.

```
"User: <users> and Group: <group>, have been se
lected"
"Using </> as the package base directory."
"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already
installed."
"## Checking for setuid/setgid programs."
"This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package."
"Do you want to continue with the installation
of <LuLUMRT> [y,n,?]"
```

8. Type y and press Return.

```
"Installing Lumos Runtime for AnyMedia NB-EM
R1.5 as <LuLUMRT>"
"## Installing part 1 of 1. "
"<files list>"
"[ verifying class <none> ]"
"## Executing postinstall script."
"You have the installation logfile in
/tmp/EM_Install_LuLUMRT.log"
"Installation of <LuLUMRT> was successful."
"Processing package instance <LuRWRT> from
<XXXXXXX>"
```

**NOTE:**

xxxxxxx shows the path where the package is installed.

```
"RogueWave Tools & Threads Runtimes for AnyMediaNBEM R1.5"
"(sparc) 7.0.7 & 1.1.2"
"OK, No previous package LuRWRT have been found."
"Enter install directory [/opt/lucent/rw] [?,q]"
```

9. Type a valid path where the package files must be placed and press Return (press Return to select default).

```
"Select owner and group for package files."
"NBR USER:GROUP"
" 1 anymedia:lucent "
" .... "
"Enter selection [?,?,q]:"
```

10. Type an user:group number and press Return.

```
"User: <users> and Group: <group>, have been selected"
"Using </> as the package base directory."
"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already installed."
"## Checking for setuid/setgid programs."
"This package contains scripts which will be executed with super-user permission during the process of installing this package."
"Do you want to continue with the installation of <LuRWRT> [y,n,?]"
```

11. Type y and press Return.

## OrbixMT 2.3c patch 02 Installation

```
"Installing RogueWave Tools & Threads Runtimes
for AnyMediaNBEM R1.5 as <LuRWRT>"

"## Installing part 1 of 1. "

"<files list>"

"[ verifying class <none> ]"

"## Executing postinstall script."

"You have the installation logfile in
/tmp/EM_Install_LuRWRT.log"

"Installation of <LuRWRT> was successful."

"Processing package instance <LuOX23RT> from
<XXXXXXX>"
```

⇒ **NOTE:**  
xxxxxxx shows the path where the package is installed.

```
"Orbix 2.3c02 Runtime for AnyMedia NB-EM R1.5"

"(sparc-solaris) Version 2.3c02MT Run-Time"

"OK, No previous package LuOX23RT have been
found."
```

⇒ **NOTE:**  
A list of partitions and free space is displayed.

```
"Here is a list of your partitions and the free
space in each of them:"

"Filesystem kbytes used avail capacity Mounted
on"

"<information about your partitions and free
space>"

"Where should Orbix be installed? [/opt/lu
cent/OrbixMT_2.3c2] [?,q] "
```

12. Type a valid path where the package files must be placed and press **Return** (press **Return** to select default).

If the DNS domain is found:

```
"The DNS domain name found was: xxxxxxxx"

"What is your DNS domain name [default: xxxxxxxx]"
```

If the DNS domain name is not found:

```
"The DNS domain name has NOT been found."
"Maybe this machine does not have DNS or is not
configured."
"If you do not have DNS then press RETURN to the
next question."
"In other case write your DNS domain name
selection or accept the default."
"What is your DNS domain name [default: ]
```

13. Type your DNS domain name and press Return (press Return to select default - available only if DNS domain was found)).

```
"Select owner and group for package files."
"NBR  USER:GROUP"
"  1  anymedia:lucent      "
"  ....  "
"Enter selection [?,?,q]:"
```

14. Type an user:group number and press Return.

```
"User: <users> and Group: <group>, have been se
lected"
"Using </> as the package base directory."
"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already
installed."
"## Checking for setuid/setgid programs."
"This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package."
"Do you want to continue with the installation
of <LuOX23RT> [y,n,?]"
```

15. Type y and press Return

```
"Installing Orbix 2.3c02 Runtime for AnyMedia
NB-EM R1.5 as <LuOX23RT>"
```

**OrbixNames 1.1c  
Installation**

```

"## Installing part 1 of 1. "
"<files list>"
"[ verifying class <bin> ]"
"<files list>"
"[ verifying class <cfg> ]"
"<files list>"
"[ verifying class <lib> ]"
"## Executing postinstall script."
"You have the installation logfile in
/tmp/EM_Install_LuOX23RT.log"
"Installation of <LuOX23RT> was successful."
"Processing package instance <LuOXNS> from
<XXXXXXX>"

```

**NOTE:**

xxxxxxx shows the path where the package is installed.

```

"OrbixNames 1.1c Runtime for AnyMedia NB-EM
R1.5"
"(sparc-solaris) Version 1.1c Run-Time"
"OK, No previous package LuOXNS have been
found."
"Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in <OrbixMT path>"
"Where should OrbixNames be installed? [/opt/lu
cent/OrbixNames1.1c][?,q] "

```

16. Type a valid path where the package files must be placed and press **Return** (press **Return** to select default).

```

"Multi-threaded Orbix installation detected, is
this correct? [y] [y,n,?] "

```

17. Type **y** and press **Return**.

```

"Select owner and group for package files."
"NBR  USER:GROUP"
"  1  anymedia:lucent      "
"  ....                  "
"Enter selection [?,?,q]:"

```



18. Type an user:group number and press Return.

```
"User: <users> and Group: <group>, have been se
lected"
"Using </> as the package base directory."
"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already
installed."
"## Checking for setuid/setgid programs."
"This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package."
"Do you want to continue with the installation
of <LuOXNS> [y,n,?]"
```

19. Type y and press Return.

```
"Installing OrbixNames 1.1c Runtime for AnyMedia
NB-EM R1.5 as <LuOXNS>"
"## Installing part 1 of 1."
"[ verifying class <names> ]"
"<files list>"
"[ verifying class <bin> ]"
"<files list>"
"[ verifying class <lib> ]"
"## Executing postinstall script."
"-----"
"Okay, OrbixNames is now installed."
"You have the installation logfile in
/tmp/EM_Install_LuOXNS.log"
"Installation of <LuOXNS> was successful."
"Processing package instance <LuOXTKRT> from
<xxxxxxx>"
```

**OrbixTalk 1.2 c  
patch02 Installation**



**NOTE:**

xxxxxxx shows the path where the package is installed.

```
"OrbixTalk 1.2c02 Runtime for AnyMedia NB-EM
R1.5"
```

```
"(sparc-solaris) 1.2c02"
```

```
"OrbixTalk Installation details:"
```

```
"Version: 1.2c02"
```

```
"Platform: Solaris 2.x"
```

```
"Compiler: WorkShop Compilers 4.2 30 Oct 1996
C++ 4.2"
```

```
"To install OrbixTalk1.2c you must already
have Orbix2.3c installed. "
```

```
"If this is not the case please exit now."
```

```
"If you already have OrbixTalk on your system,
this installation may overwrite some of the
files. Make sure you have a backup of your old
OrbixTalk, or install this new version in a new
set of directories. If you want to make a backup
copy of the old version, you should exit now."
```

```
"It is recommended that you read the installa
tion guide before you continue."
```

```
"Do you want to continue? [y]:"
```

20. Type **y** and press **Return**.

```
"OK, No previous package LuOXTKRT have been
found."
```

```
"Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in <OrbixMT path>"
```



#### NOTE:

A list of partitions and free space is displayed.

```
"Here is a list of your partitions and the free
space in each of them:"
```

```
"Filesystem kbytes used avail capacity Mounted
on"
```

```
"<information about your partitions and free
space>"
```

```
"Where should the main OrbixTalk software dis
tribution be installed?[/opt/lu
cent/OrbixTalk1.2c02] "
```

21. Type a valid path where the package files must be placed and press Return (press Return to select default).
 

```
"Which UDP/IP port should the OrbixTalk Directory Enquiries daemon use?"
"OrbixTalk requires that you reserve a range of
AT LEAST 2 ports starting at this port? [5xxx]"
```
22. Type a valid UDP/IP port and press Return (press Return to select default).
 

```
"The OrbixTalk Directory Enquiries daemon assigns individual Topics an IP Multicast address starting with the next address above the base IP address. What base IP Multicast address ( within the range 225.0.0.0 to 239.255.255.255 ) should the OrbixTalk Directory Enquiries daemon use?[225.0.0.0]"
```
23. Type a valid IP multicast address and press Return (press Return to select default).
 

```
"What directory should the OrbixTalk data files be stored? [/opt/lucent/OrbixTalk1.2c02/dat]"
```
24. Type a valid path (for instance <OrbixTalk path>/dat where the package files must be placed and press Return (press Return to select default).
 

```
"Select owner and group for package files."
"NBR  USER:GROUP"
"  1  anymedia:lucent      "
"  ....  "
"Enter selection [?,?,q]:"
```
25. Type an user:group number and press Return.
 

```
"User: <users> and Group: <group>, have been selected"
"Using </> as the package base directory."
"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already installed."
```

```

"## Checking for setuid/setgid programs."

"This package contains scripts which will be executed with super-user permission during the process of installing this package."

"Do you want to continue with the installation of <LuOXTKRT> [y,n,?]"

```

26. Type **y** and press Return.

```

"Installing OrbixTalk 1.2c02 Runtime for AnyMedia NB-EM R1.5 as <LuOXTKRT>"

"## Installing part 1 of 1. "

"<files list>"

"[ verifying class <bin> ]"

"<files list>"

"[ verifying class <lib> ]"

"<files list>"

"[ verifying class <raw> ]"

"## Executing postinstall script."

"* Making backing copy of the orbix configuration file <OrbixMT path>/cfg/Orbix.cfg" to "<OrbixMT path>/cfg/Orbix.cfg.old"

"* Licence registration was accepted for otd."
"* Licence registration was accepted for otmsd."
"* Licence registration was accepted for otdsm."
"*****"
"*  INSTALLATION WARNINGS:"
""

"* For Orbix and OrbixTalk to be able to find Orbix.cfg, you must set the environment variable IT_CONFIG_PATH to its location, ie. "<OrbixMT path>/cfg/Orbix.cfg"."

"* If the OrbixTalk binaries fail with the message "password" invalid"

"The licence install utility will need to be run manually. Enter the following command: "

" <OrbixMT path>/bin/install_licence <OrbixTalk path>/bin/otd <code>"

```

**ObjectStore 5.0 Installation**

```

"* OrbixTalk 1.2c02 is now successfully in
stalled."

"You have the installation logfile in
/tmp/EM_Install_LuOXTKRT.log"

"Installation of <LuOXTKRT> was successful."

"Processing package instance <LuOSRT> from
<XXXXXXX>"

```

**NOTE:**

xxxxxxx shows the path where the package is installed.

```

"ObjectStore 5.0_SP3 Runtime for AnyMedia NB-EM
R1.5"

"(sparc-solaris) 5.0_SP3 Run-Time"

"Enter install directory [/opt/lucent/OS50_SP3]
[?,q]"

```

27. Type a valid path where the package files must be placed and press Return (press Return to select default).

```

"Using </> as the package base directory."

"## Processing package information."

"## Processing system information."

"## Verifying disk space requirements."

"## Checking for conflicts with packages already
installed."

"## Checking for setuid/setgid programs."

"The following files are being installed with
setuid and/or setgid permissions: <ObjectStore
path>/sunpro/lib/oscmnit <setuid root>"

"Do you want to install these as setuid/setgid
files [y,n,?,q]"

```

28. Type y and press Return.

```

"This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package."

"Do you want to continue with the installation
of <LuOSRT> [y,n,?]"

```

29. Type y and press Return.

```
"Installing ObjectStore 5.0_SP3 Runtime for Any
Media NB-EM R1.5 as <LuOSRT>"
```

```
"## Installing part 1 of 1. "
```

```
"<files list>"
```

```
"[ verifying class <none> ]"
```

```
"## Executing postinstall script."
```

```
"*****"
```

```
" * Remember execute "osconfig" to set the envi
ronment *"
```

```
"*****"
```

```
" You have the installation logfile in
/tmp/EM_Install_LuOSRT.log"
```

```
"Installation of <LuOSRT> was successful."
```

## ObjectStore Configuration

```
"Object Store configuration"
```

```
"The default copy of ObjectStore to configure is
in <ObjectStore path>/sunpro."
```

```
"Is this the copy that you want to configure?
[yes]"
```

30. Press Return.

```
"ObjectStore includes shared libraries. For Ob
jectStore applications and utilities to work,
the dynamic linker must be able to find them."
```

```
"The recommended arrangement is to have symbolic
links in /usr/lib to the shared libraries."
```

```
"If you choose not to make these links, then you
will have to instruct all ObjectStore users to
add <ObjectStore path>/sunpro/lib to their
LD_LIBRARY_PATH environment variable."
```

```
"Do you want to create links to ObjectStore li
braries in /usr/lib? [yes]"
```

31. Press Return.

```
"Since you have requested a File-database con
figuration, you must give a pathname for the
transaction log file. Where do you want to put
the transaction log?"
```

32. Type `<AnyMedia_Absolute_PATH>/DBTrxLog/transaction.log` and press Return or type `<path of the separate partition created for the transaction log file (cf. page 2)>/transaction.log` and press Return.

"You have configured this machine to run an ObjectStore server. The server's transaction log is in `<Transaction log path>`."

"Do you want to proceed? [yes]"

33. Press Return.

"Writing configuration files and initializing the server, please"

"wait..."

"990423 111330 ObjectStore Release 5.0 Service Pack 3 Database Server"

"ObjectStore includes a server daemon which must be running for any application to access an ObjectStore database."

"It is recommended that you auto-start the daemon via commands in your operating system startup scripts. If you do not configure automatic startup, you will have to start the server daemon by hand, or re-run this utility to configure auto-start."

"Would you like to configure automatic server startup and shutdown? [yes]"

34. Type No and press Return.

"This script will now verify the installation:"

"The ObjectStore Server daemon process is accessible. Schema databases are accessible."

"The cache manager launcher for release 4 (`<ObjectStore path>/sunpro/lib/oscmunit`) has correct modes and ownership."

"ObjectStore configuration completed."

"Package to be installed: LuANY15S"

"Processing package instance `<LuANY15S>` from `<XXXXXXX>`"

### **AnyMedia Servers Installation**

**NOTE:**

xxxxxxx shows the path where the package is installed.

```
"AnyMedia NB Element Manager Release 1.5
(server)"

"(sparc) LuANY15S_X.Xc"

"*****"

"*AnyMedia Element Manager *"

"*(c) 1999-Lucent Technologies *"
"*****"

"OK, No previous package LuANY15S have been
found."

"***Select an installation path for AnyMediaEM
R1.5 server applications***"

"Enter install directory for the AnyMediaEM
R1.5 [/opt/lucent/AnyMediaNBEM_R1.5] [?,q] "
```

35. Type a valid path where the package files must be placed and press Return (press Return to select default).

```
"The installation path selected for AnyMedia EM
R1.5 is <Server path>"

"Package <LuOX23RT> OrbixMT Version 2.3c02MT
Run-Time have been found in <OrbixMT path>"

"Package <LuOXTKRT> OrbixTalk 1.2c02 have been
found in <OrbixTalk path>"

"Package <LuOXTKRT> OTGateway 2.0c02-01 have
been found in <OrbixTalk path>"

"Package <LuOXNS> OrbixNames Version 1.1c Run-
Time have been found in <OrbixNames path>"

"Package <LuOSRT> ObjectStore 5.0_SP3 Run-Time
have been found in <ObjectStore path>"

"Package <LuLUMRT> Lumos Build 5 run-time have
been found in <Lumos path>"

"Package <LuRWRT> RogueWave Tools and Threads
7.0.7 & 1.1.2 have been found in <RogueWave
path>"

"Select owner and group for package files."

"NBR USER:GROUP"
```



```
" 1 anymedia:lucent "
```

```
" .... "
```

```
"Enter selection [?,?,q]:"
```

36. Type a user:group number and press Return.

```
"User: <users> and Group: <group>, have been selected"
```

```
****Boot processes****
```

```
"Do you like install the SystemAdmin process on the system boot [y,n,?,q]"
```

37. Type **y** to confirm and press Return or type **n** to do nothing on the system.



**NOTE:**

If you select **y** the following request is displayed.

```
"Start-up MODE"
```

```
" 1 ALL to start-up all AnyMedia applications"
```

```
" 2 CORE to start-up only core AnyMedia applications"
```

```
"Enter selection [?,?,q]:"
```

38. Type the desired Start-up mode < 1 or 2 >

```
*****cron processes*****
```

```
"RemoveAlm cron process will be executed every day at 3.00 AM. Do you like change it [y,n,?,q]"
```

39. Type **y** to confirm and press Return or type **n** and press Return to do nothing on the system.



**NOTE:**

If you select **y** the following requests are displayed.

```
"Enter minute (0-59,*): [?,q]"
```

40. Type a valid entry.

```
"Enter hour (0-23,*): [?,q]"
```

41. Type a valid entry

```
"Enter day of the month (1-31,*): [?,q]"
```

42. Type a valid entry.

```
"Enter month of the year (1-12,*):  [?,q]"
```

43. Type a valid entry.

```
"Enter day of the week (0-6 with 0=Sunday,*):  
[?,q]"
```

44. Type a valid entry.

```
"Do you like install the Backup process as a  
cron [y,n,?,q]"
```

45. Type **y** to confirm and press **Return** or type **n** and press **Return** to do nothing on the system.



**NOTE:**

If you select **y** refer to steps 40 - 44.

```
"Do you like install the Archive process as a  
cron [y,n,?,q]"
```

46. Type **y** to confirm and press **Return** or type **n** and press **Return** to do nothing on the system.



**NOTE:**

If you select "**y**" refer to steps 40 - 44.

```
"Clean-up tasks for the AnyMediaNB-EM system  
will be executed every"
```

```
"day at 4.00 AM. Do you like change it  
[y,n,?,q]"
```

47. Type **y** to confirm and press **Return** or type **n** and press **Return** to do nothing on the system.



**NOTE:**

If you select **y** refer to steps 40 - 44.

```
"Using </> as the package base directory."
```

```
"## Processing package information."
```

```
"## Processing system information."
```

```
"## Verifying disk space requirements."
```

```
"## Checking for conflicts with packages already  
installed."
```

**NOTE:**

If the transaction.log was installed inside the AnyMedia tree (default) there is an attribute conflict and the following question is displayed:

```
"The following files are already installed on
the system and are being used by another pack-
age:"
```

```
"*/opt/lucent/AnyMediaNBEM_R1.3 <attribute
change only>"
```

```
"* - conflict with a file which does not belong
to any package"
```

```
"Do you want to install these conflicting files
[y,n,?,q]"
```

48. Type **y** and press Return.

```
"## Checking for setuid/setgid programs."
```

```
"This package contains scripts which will be ex-
ecuted with super-user permission during the
process of installing this package."
```

```
"Do you want to continue with the installation
of <LuANY15S> [y,n,?]"
```

49. Type **y** and press Return.

```
"Installing AnyMedia NB Element Manager Release
1.5 (server) as <LuANY15S>"
```

```
"## Installing part 1 of 1. "
```

```
"<files list>"
```

```
"[ verifying class <common> ]"
```

```
"<files list>"
```

```
"[ verifying class <channels_30> ]"
```

```
"## Executing postinstall script."
```

```
"Starting orbixd daemon in the system"
```

```
"Starting ns daemon in the system"
```

```
"[ s1224: OrbixNames (Release 1.1) ]"
```

```
"[ s1369: OrbixOTM package (Release 1.0) ]"
```

```
"Checking AnyMedia EM R1.5 naming contexts"
```

```
"Starting CreateNEM_db process..."
```

```
"Getting the AnyMedia installation path..."
```

```
"OK"
"Getting NEM data base path"
"OK"
"Creating NEM Data Base"
"OK"
"exit OK"
"Starting CreateCMR12_db process..."
"Getting the AnyMedia installation path..."
"OK"
"Getting CM R1.2 data base path"
"OK"
"Creating CM R1.2 Data Base"
"OK"
"exit OK"
"Starting AMDbPopulate process..."
"Getting the AnyMedia installation path..."
"OK"
"Getting Alarm data base path"
"OK"
"Creating Alarm Data Base..."
"Creating os_Collection<HostElement*>..."
"Creating ListOfAlarmsPerHost ..."
"Creating segment and ElementManager Host
(0)..."
"OK"
"exit OK"
"Getting the AnyMedia installation path..."
"Getting OAM Security data base path"
"OK"
"Creating Database"
"Registering Servers in the Orbix Implementation
Repository"
""
"[20948: New Connection"
"(<hostname>. <domain_name>, IT_daemon,*,root,
pid=<pid>,optimised) ]"
```

```

"[20949: New Connection"
"(<host name>.<domain_name>,IT_daemon, *,root
,pid=<pid>,optimised) ]"
"[20950: New Connection"
...
"<pid> Killed"
"orbixd daemon pid=<pid> have been killed. Was
mine."
"20846 Killed"
"ns daemon pid=20846 have been killed. Was
mine."
*****
"* Execute ". AnyMediaNBEM.sh" to set the envi
ronment *"
*****
"You have the installation logfile in <Server
path>/tmp/EM_Install.log"
"Installation of <LuANY15S> was successful."
"Installation of AnyMedia EM R1.5 was successful
<Server side installation>"

```

50. Reboot the machine in order to activate the cron and configuration files.

### 2.2.1.2 Client Side Installation

Complete the following procedure to install the *AnyMedia* client side.

Step	Procedure
51.	Go to the directory where the installation script is placed (cdrom or disk).
52.	Type <code>./install_AMEMR15</code> and press Return.
	<pre> AnyMedia NB EM R1.5 installation CopyRight (c) 1999 Lucent Technologies, Inc. All Rights Reserved  **Pre-requisites**  1.- Before attempting to install the applica tion, please,read the readme.txt file. </pre>

2.- AnyMedia NB EM R1.5 runs on SUN SPARC Solaris 2 computers running Solaris 2.5.1 plus security and Y2000 patches recommended by SUN and 106255-01 patch.

3.- TCP ports:

The following ports MUST be available in order to successfully run the AnyMedia EM:

\* 1570: Orbix daemon uses the TCP port 1570 in order to wait for incoming connections that use the Orbix protocol.

\* 1591 to 1641: As Corba servers are activated by the Orbix daemon, they are assigned a port so that clients can communicate with it.

\* OrbixTalk uses two ports for communications. These ports have as default values "5000" and the next one. The first can be modified at installation time to a value between 1024 and

65534. It is essential that these ports are not used by any process on the SAME SUBNET DOMAIN.

4.- IP multicast addresses:

Using OrbixTalk, all communications takes place using multicast addresses. The range of IP multicast addresses used by OrbixTalk is 31 with 255.0.0.0 as the first IP address (it is configurable at installation time in the range 255.0.0.0 to 239.255.255.255)

5.- The install\_AMEMR15 script runs on K-shell <ksh> environment.

6.- The time zone MUST be the same for the Any Media Client <GUI>, LUMOS and Network Element. This parameter is needed for installing the Any Media Client.

\*\*\*\*\*

Do you like to continue [y,n,?,q]

53. Type **y** and press Return to continue or type **n** or **q** and press Return to exit.

"AnyMedia NB EM R1.5 installation"

"Copyright (c) 1999 Lucent Technologies, Inc."

"All Rights Reserved."

"Please, choose the installation mode"

" 1 Client <Client side installation>"

```
" 2 Server      <Server side installation>"
"Enter selection [?,??,q]:"
```

54. Type 1 and press Return.

jre 1.1.7 + symantec  
classes + reportPro  
class Installation

```
"Packages to be installed: LuJRERT, LuOXWRT,  
LuANY15en, LuANY15C"
```

```
"Processing package instance <LuJRERT> from  
<XXXXXXX>"
```



NOTE:

xxxxxxx shows the path where the package is installed.

```
"JRE 1.1.7 for AnyMediaNBEM R1.5"
"(sparc-solaris) 1.1.7"
"OK, No previous package LuJRERT have been  
found."
"Applications to install:"
"1 --> jre version 1.1.7"
"2 --> symantec classes"
"3 --> report pro classes"
"4 --> all"
"5 --> exit"
"Selection:"
```

55. Type 4 and press Return.

```
"Enter install directory [/opt/lucent/jre1.1.7]  
[?,q] "
```

56. Type a valid path where the package files must be placed and press Return (press Return to select default).

```
"Select owner and group for package files."
"NBR  USER:GROUP"
" 1  anymedia:lucent      "
" .... "
"Enter selection [?,??,q]:"
```

57. Type an user:group number and press Return.

```

"User: <users> and Group: <group>, have been se
lected"

"Using </> as the package base directory."

"## Processing package information."

"## Processing system information."

"## Verifying disk space requirements."

"## Checking for conflicts with packages already
installed."

"## Checking for setuid/setgid programs."

"This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package."

"Do you want to continue with the installation
of <LuJRERT> [y,n,?]"

```

58. Type **y** and press Return.

```

"Installing JRE 1.1.7 for AnyMediaNBEM R1.5 as
<LuJRERT>"

"## Installing part 1 of 1. "

"<files list>"

"[ verifying class <jre> ]"

"<files list>"

"[ verifying class <symantec> ]"

"<files list>"

"[ verifying class <report> ]"

"## Executing postinstall script."

"You have the installation logfile in"

"/tmp/EM_Install_LuJRERT.log"

"Installation of <LuJRERT> was successful."

```

#### OrbixWeb 3.0 In- stallation

```

"Processing package instance <LuOXWRT> from
<XXXXXXX>"

```



#### NOTE:

xxxxxxx shows the path where the package is installed.

```

"OrbixWeb 3.0 Runtime for AnyMedia NB-EM R1.5"

"(sparc-solaris) Version 3.0 Run-Time"

```



```
"Installing Version 3.0 Run-Time."
```

```
"OK, No previous package LuOXWRT have been found."
```

```
"Enter install directory [/opt/lucent/OrbixWeb3.0] [?,q]"
```

59. Type a valid path where the package files must be placed and press **Return** (press **Return** to select default).

```
"Package <LuJRERT> jre 1.1.7 have been found in <jre Path>"
```

If the DNS domain is found:

```
"The DNS domain name found was: xxxxxxxx"
```

```
"What is your DNS domain name [default: xxxxxxxx]"
```

If the DNS domain name is not found:

```
"The DNS domain name has NOT been found."
```

```
"Maybe this machine does not have DNS or is not configured."
```

```
"If you do not have DNS then press RETURN to the next question."
```

```
"In other case write your DNS domain name selection or accept the default."
```

```
"What is your DNS domain name [default: ]"
```

60. Type your DNS domain name and press **Return** (press **Return** to select default - available only if DNS domain was found)).

```
"Enter the NS hostname? [hostname] [?,q]"
```

61. Type the AEM-NB server hostname and press **Return** or accept the default hostname by pressing **Return** only.

```
"Do you agree with NS hostname? [<hostname> <IP address>] [y,n,?,q]:"
```

62. Type **y** and press **Return** if the IP address is correct.

```
"Select owner and group for package files."
```

```
"NBR USER:GROUP"
```

```
" 1 anymedia:lucent "
```

```
" .... "
```

```
"Enter selection [?,?,q]:"
```

63. Type an user:group number and press Return.

```
"User: <users> and Group: <group>, have been se
lected"

"Using </> as the package base directory."

"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already
installed."
"## Checking for setuid/setgid programs."

"This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package."

"Do you want to continue with the installation
of <LuOXWRT> [y,n,?]"
```

64. Type y and press Return.

```
"Installing OrbixWeb 3.0 Runtime for AnyMedia
NB-EM R1.5 as <LuOXWRT>"

"## Installing part 1 of 1. "

"<files list>"

"[ verifying class <none> ]"

"## Executing postinstall script."

" You have the installation logfile in
/tmp/EM_Install_LuOXWRT.log"

"Installation of <LuOXWRT> was successful."
```

#### Netscape 4.51 In- stallation

```
"Processing package instance <LuNETSCP> from
<tmp>"

"Netscape Navigator 4.51 (Stand Alone) for
AnyMedia NB-EM R1.3 (sparc-solaris) Version 4.51"

"OK, No previous package LuNETSCP have been
found."

"Enter install directory?
[/opt/lucent/Netscape] [?,q]"
```

65. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
"Select owner and group for package files."
"NBR  USER:GROUP"
"  1  anymedia:lucent      "
"  ....  "
"Enter selection [?,?,q]:"
```

66. Type an user:group number and press **Return**.

```
"User: <users> and Group: <group>, have been selected"
"Using </> as the package base directory."
"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already installed."
"## Checking for setuid/setgid programs."
"This package contains scripts which will be executed with super-user permission during the process of installing this package."
"Do you want to continue with the installation of <LuNETSCP> [y,n,?]"
```

67. Type **y** and press **Return**.

```
"Installing Netscape Navigator 4.51 (Stand Alone) for AnyMedia NB-EM R1.3 as <LuNETSCP>"
"## Installing part 1 of 1. "
"<files list>"
"[ verifying class <common> ]"
"## Executing postinstall script."
"You have the installation logfile in"
"/tmp/EM_Install_LuNETSCP.log"
"Installation of <LuNETSCP> was successful."
```

**AnyMedia Help Installation**

```
"Processing package instance <LuANY15en> from
<XXXXXXX>"
```

**NOTE:**

xxxxxxx shows the path where the package is installed.

```
"AnyMedia NB Element Manager Release 1.5 (Help)"
"(sparc) LuANY15en_US_X.X"
" *****"
" *          AnyMedia Element Manager*"
" *          (c) 1999-Lucent Technologies*"
" *****"
"OK, No previous package LuANY15en have been
found."
"Where should AnyMediaNBEM Help be installed?
[/opt/lucent/AnyMediaNBEM_R1.5/Help] [?,q]"
```

68. Type a valid path where the package files must be placed and press **Return** or press **Return** to accept the default path.

```
"Select owner and group for package files."
"NBR  USER:GROUP"
"  1  anymedia:lucent      "
"  ....                  "
"Enter selection [?,?,q]:"
```

69. Type an user:group number.

```
"User: <users> and Group: <group>, have been se
lected"
"Using </> as the package base directory."
"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already
installed."
"## Checking for setuid/setgid programs."
```

```
"This package contains scripts which will be executed with super-user permission during the process of installing this package."
```

```
"Do you want to continue with the installation of <LuANY15en> [y,n,?]"
```

70. Type **y** and press **Return**.

```
"Installing AnyMedia NB Element Manager Release 1.5 (Help) as <LuANY15en>"
```

```
"## Installing part 1 of 1. "
```

```
"<files list>"
```

```
"[ verifying class <common> ]"
```

```
"## Executing postinstall script."
```

```
"You have the installation logfile in"
```

```
"/tmp/EM_Install_LuANY15en.log"
```

```
"Installation of <LuANY15en> was successful."
```

### **AnyMedia Client Installation**

```
"Processing package instance <LuANY15C> from <xxxxxxx>"
```



#### **NOTE:**

xxxxxxx shows the path where the package is installed.

```
"AnyMedia NB Element Manager Release 1.5 (Client)"
```

```
"(sparc) <LuANY15C_X.Yc>"
```

```
" *****"
```

```
" * AnyMedia Element Manager*"
```

```
" * (c) 1999-Lucent Technologies*"
```

```
" *****"
```

```
"OK, No previous package LuANY15C have been found."
```

```
"Where should AnyMediaNBEM GUI be installed? [/opt/lucent/AnyMediaNBEM_R1.5/GUI] [?,q] "
```

71. Type a valid path where the package files must be placed and press **Return** (press **Return** to select default).

```
"Package <LuOXWRT> OrbixWeb Version 3.0 Run-Time
have been found in <OrbixWeb path>"
```

```
"Package <LuJRERT> jre 1.1.7 have been found in
<jre path>"
```

```
"Package <LuANY15en> Help have been found in
<Help path>"
```

```
"Package <LuNETSCP> have been found in
<Netscape path>"
```

```
"Select owner and group for package files."
```

```
"NBR  USER:GROUP"
```

```
"  1  anymedia:lucent      "
```

```
"  ....  "
```

```
"Enter selection [?,?,q]:"
```

72. Type an user:group number.

```
"User: <users> and Group: <group>, have been se
lected"
```

```
"What is the AnyMediaNBEM Server Host? [<de
fault>] [?,q] "
```

73. Type the host name where the *AnyMedia* AEM-NB servers were installed and press Return (press Return to select default).

```
"Wait...."
```

```
"What is the URL for Broad Band Manager?
[http://www.lucent.com][?,q]"
```

74. Type a valid URL where the broad band manager is placed and press Return (press Return to select default).

```
"Login for CutThrough functionality? [?,q]"
```

75. Type a valid login and press Return.

```
"Password for CutThrough functionality? [?,q]"
```

76. Type a valid password and press Return.

```
"The name of the location where the EM is work-
ing is needed for printing facility."
```

"What is the name of the location?"

The location name will appear in the document header of the printing facility.

77. Type your AEM-NB location name and press **Return**.

"Code for the representation of names of languages"

"Refer to ISO 639:1988 (E/F) for more information"

" 1 da Danish"

" 2 de German"

" 3 fr French"

" 4 it Italian"

" 5 zh Chinese"

" 6 es Spanish"

" 7 en English"

"Enter selection [?,??,q]:"

78. Type your language code and press **Return**.

"Code for the representation of names of countries"

"Refer to ISO 3166 for more information"

" 1 DK DENMARK"

" 2 DE GERMANY"

" 3 FR FRANCE"

" 4 IT ITALY"

" 5 CN CHINA"

" 6 ES SPAIN"

" 7 GB UNITED KINGDOM"

" 8 US UNITED STATES"

"Enter selection [?,??,q]:"

79. Type your country code and press **Return**.

"Code for the representation of names of Time Zones"

" 1 GMT (0) Greenwich Mean Time"

```

" 2 ECT      (1)    European Central Time"
" 3 EET      (2)    Eastern European Time"
" 4 ART      (2)    (Arabic) Egypt Standard
                    Time"
" 5 EAT      (3)    Eastern African Time"
" 6 MET      (3.5)  Middle East Time"
" 7 NET      (4)    Near East Time"
" 8 PLT      (5)    Pakistan Lahore Time"
" 9 IST      (5.5)  India Standard Time"
" 10 BST     (6)    Bangladesh Standard Time"
"... 21 more menu choices to follow;"
"<RETURN> for more choices, <CTRL-D> to stop
display:"
"Enter selection [?,??,q]:"

```

80. Type the desired time zone and press Return.



**NOTE:**

The time zone **must** be the same for the *AnyMedia* Client (GUI), LUMOS, Network Element and OS.

```

"Using </> as the package base directory."
"## Processing package information."
"## Processing system information."
"## Verifying disk space requirements."
"## Checking for conflicts with packages already
installed."
"## Checking for setuid/setgid programs."
"This package contains scripts which will be ex
ecuted with super-user permission during the
process of installing this package."
"Do you want to continue with the installation
of <LuANY15C> [y,n,?]"

```

81. Type **y** and press Return.

```

"Installing AnyMedia NB Element Manager Release
1.5 (Client) as <LuANY15C>"

```



```
### Installing part 1 of 1. "  
<files list>"  
[ verifying class <common> ]"  
### Executing postinstall script."  
  
*****  
* Execute ". AnyMediaNBEM_GUI.sh" to set the  
environment *  
*****  
" You have the installation logfile in <Client  
path>/EM_Install.log"  
"Installation of <LuANY15C> was successful."  
  
"Installation of AnyMedia EM R1.5 was successful  
<Client side installation>"
```

### 2.2.1.3 Post-Install Actions

#### 2.2.1.3.1 AEM-NB Server

To be able to start-up the server it is necessary previously to execute the following script:

**". <AnyMedia\_path>/cfg/AnyMediaNBEM.sh"**

This would set all the necessary environment variables. It is recommended to include this line in the user .profile or to create an alias to facilitate the use.

#### 2.2.1.3.2 AEM-NB Client

To be able to start-up the GUI it is necessary previously to execute the following script:

**". <AnyMedia\_path>/GUI/AnyMediaNBEM\_GUI.sh"**

This would set all the necessary environment variables. It is recommended to include this line in the user .profile or to create an alias to facilitate the use.

### 2.2.2 Installing Individual Packages

Also, it is possible to install each package individually using the command **pkgadd -d <path\_name> package\_name** (refer to Table 2-1, page 2-4 to obtain the packages names) or using the **admintool** (system administration with a graphical interface). In case you have to do an individual server package installation, then after you have finished, reboot the machine.

#### NOTE:

If the package is already installed on the target system, the following actions must be done:

- the package must be de-installed previously (refer to "Remove Any-Media Package Installations" on page 43 for more information about packages de-installation)
- in order not to affect the rest of the installed packages, the package must be re-installed in the same directory as the previous one.

For this type of installation it is necessary to comply with the packaged dependences showed in the following table.

**Table 2-2 Packages Dependences**

To install	the following package must be installed previously
OrbixNames	OrbixMT
OrbixTalk	OrbixMT
OrbixWeb	jre

**Table 2-2 Packages Dependences**

To install	the following package must be installed previously
<i>AnyMedia</i> Servers	OrbixMT
	OrbixTalk
	OrbixNames
	LUMOS
	ObjectStore
	RogueWave
<i>AnyMedia</i> Client	OrbixWeb
	jre + symantec + reportPro
	Netscape
Help	none

System responses and inputs for this type of installation and for a full installation are similar. Only the following differences could be found:

- When an installation starts, the package checks if a previous installation of the package already exists in the system. If no previous package is found, the following message will appear:

**"OK, No previous package <Package\_Name> have been found."**

**NOTE:**

Refer to "Type 2 and press Return" on page 8 to see this response.

If one of the following messages appears, the installation will stop without changes on the system:

- The following message appears if there is a previous package in the system that was completely installed and has the same version
 

**"Previous completely installed package <Package\_Name> version: <Package\_Version> have been found. And it is the same to the new one you want to install:<Package\_Version>."**
- The following message appears if there is a previous package in the system that was partially installed and has the same version
 

**"Previous partially installed package <Package\_Name> version: <Package\_Version> have been found. And it is the same to the new one you want to install:<Package\_Version>. But it is partially installed. Better to use pkgmgr <Package\_Version> and installed it again."**

- The following message appears if there is a previous package in the system that was (partially or completed) installed and has different version
 

```
"Current administration requires that a unique instance of the <Package_Name> package be created. However, the maximum number of instances of the package which may be supported at one time on the same system has already been met. No changes were made to the system"
```

After this step, the installation looks for its packages dependencies. If a needed package is found the following message will appear:

```
"Package <Package_Name> <Application_Name>
<Application_Version> have been found in
<Application_Path>"
```



**NOTE:**

Refer to "Type y and press Return" on page 13 to see this response.

If the package is not found, the installation will prompt about its installation path in order to check this path and the correct application version:

```
"<Package_Name> needs <Application_Name>
<Application_Version> to be installed previously. If it isn't, Answer 'q' to next question and install the package <Package_Name> otherwise provide the paths required.
```

```
What is the base path of <Required_Package_Name>
<Package_version> [?,q]?"
```

When an input is provided the installation checks the path and the version of the application. If the path is invalid the following message will appear:

```
"ERROR: Pathname does not exist."
```

If the version is invalid one of the following messages could appear:

```
"Package <Required_Package_Name> have been found
but INSTALL_PATH is not defined"
```

```
"Package <Required_Package_Name> have been found
but with version: <Package_Version> not valid
for <Package_Name>"
```

In both cases, the installation will prompt again for the required package.

- Also, the path where the Orbix.cfg file is located is requested in the OrbixNames, OrbixTalk and AnyMedia Servers packages installation, after the request for the installation path of the OrbixMT -the file will be modified by both installations- :

```
"Where is Orbix.cfg file located
[Orbix_path/cfg] [?, ??, q]?"
```

- Finally, after the ObjectStore installation the user must execute the `osconfig server` command, to configure the ObjectStore daemon (refer to steps 30 to 41).

### 2.2.3 Cancel Installation

There are two ways to cancel the installation, as follows:

- internal cancellation: when the `install_AMEMR15` or `pkgadd` command detect through information files or installation scripts that something is invalid.
- external cancellation: if the administrator kill the process (kill -9 or Ctrl+C).

In both cases, the `system` informs about if files have been installed on the system. In this case, the administrator must use the `pkgrm` command to remove the installation.

### 2.2.4 Remove AnyMedia Package Installations

In order to remove any *AnyMedia* package installations, the administrator must execute the command `pkgrm <Package_Name>`.



#### NOTE:

Refer to Table 2-1, page 2-4 to obtain the *AnyMedia* packages names.

When a package is removed, all files installed by it or created during the *AnyMedia* operation, such as data bases and temporal data files, are erased in the target system.

#### 2.2.4.1 Remove AnyMedia Servers Package

Complete the following procedure to remove the *AnyMedia* Servers package.

Step	Procedure
------	-----------

- |    |  |
|----|--|
| 1. | Log in as <code>root</code> .                                    |
| 2. | Type <code>pkgrm LuANY15S</code> and press <code>Return</code> . |

The following package is currently installed:

```
LuANY15S      AnyMedia NB Element Manager Release
               1.5 (server)(sparc) LuANY15S_X.Xc
Do you want to remove this package?
```

3. Type **y** and press Return.

```
## Removing installed package instance
<LuANY15S>

This package contains scripts which will be
executed with super-user permission during the
process of removing this package.

Do you want to continue with the removal of this
package [y,n,?,q]
```

4. Type **y** and press Return.

```
## Verifying package dependencies.
## Processing package information.
## Executing preremove script.
Removing data bases
TRACE: Removing NEM data base
TRACE: Removing CM data base
TRACE: Removing ALM data base
TRACE: Removing SEC data base
## Removing pathnames in class <channels_30>
## Removing pathnames in class <common>
<files list>
## Executing postremove script.
## Updating system information.
Removal of <LuANY15S> was successful.
```

You have now removed the *AnyMedia* Servers package.

#### 2.2.4.2 Remove *AnyMedia* Client Package

Complete the following procedure to remove the *AnyMedia* Client package.

Step	Procedure
------	-----------

1. Log in as **root**.
2. Type **pkgrm LuANY15S** and press Return.

```
The following package is currently installed:
LuANY15C    AnyMedia NB Element Manager Release
            1.5 (Client) (sparc) LuANY15C_X.Xc
```

Do you want to remove this package?

3. Type **y** and press Return.

```
## Removing installed package instance  
<LuANY15C>
```

This package contains scripts which will be executed with super-user permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q]

4. Type **y** and press Return.

```
## Verifying package dependencies.  
## Processing package information.  
## Executing preremove script.  
## Removing pathnames in class <channels_30>  
## Removing pathnames in class <common>  
<files list>  
## Executing postremove script.  
## Updating system information.  
Removal of <LuANY15C> was successful
```

You have now removed the *AnyMedia* Client package.

### 2.2.4.3 Remove Third-Party Packages

The following procedure is the same for all parts of the Third-Party software. For example the procedure below describes the removal of the RogueWave package.

Complete the following procedure to remove the RogueWave package:

Step	Procedure
1.	Log in as <code>root</code> .
2.	Type <code>pkgrm LuRWRT</code> and press <code>Return</code> .  The following package is currently installed: LuRWRT RogueWave Tools & Threads Runtimes for AnyMediaNBEM R1.5 (sparc) 7.0.7 & 1.1.2 Do you want to remove this package?
3.	Type <code>y</code> and press <code>Return</code> .  ## Removing installed package instance <LuRWRT> ## Verifying package dependencies. ## Processing package information. ## Removing pathnames in class <none> <file list> ## Updating system information. Removal of <LuRWRT> was successful.

You have now removed the RogueWave package.



---

## Contents

<b>3.1</b>	<b>Overview</b>	<a href="#"><u>3-1</u></a>
<b>3.2</b>	<b>System Access</b>	<a href="#"><u>3-2</u></a>
3.2.1	Login to Operation System	<a href="#"><u>3-2</u></a>
3.2.2	Logout from Operation System	<a href="#"><u>3-3</u></a>
3.2.3	AEM-NB Access Bar	<a href="#"><u>3-4</u></a>
3.2.3.1	Alarm Notification Icon	<a href="#"><u>3-4</u></a>
3.2.3.2	Help Icon	<a href="#"><u>3-5</u></a>
3.2.4	Capacity	<a href="#"><u>3-5</u></a>
<b>3.3</b>	<b>General Information on Keyboard and Windows</b>	<a href="#"><u>3-6</u></a>
3.3.1	Keyboard	<a href="#"><u>3-6</u></a>
3.3.2	Mouse	<a href="#"><u>3-6</u></a>
3.3.3	Different Aspects of the Cursor	<a href="#"><u>3-7</u></a>
3.3.4	Basics on Windows	<a href="#"><u>3-7</u></a>
3.3.5	Window Menu	<a href="#"><u>3-10</u></a>
3.3.6	Menu Bar	<a href="#"><u>3-11</u></a>
3.3.7	Cursor Menu	<a href="#"><u>3-11</u></a>
3.3.8	Workspace Manager	<a href="#"><u>3-12</u></a>
3.3.9	Workspace Menu	<a href="#"><u>3-12</u></a>
3.3.10	Controls in AEM-NB Windows	<a href="#"><u>3-13</u></a>
<b>3.4</b>	<b>Application Start-Up and Shutdown</b>	<a href="#"><u>3-17</u></a>
3.4.1	General on Applications	<a href="#"><u>3-17</u></a>
3.4.2	AEM-NB Server Applications	<a href="#"><u>3-18</u></a>
3.4.3	Start-Up/Shutdown of Server Applications via GUI	<a href="#"><u>3-18</u></a>
3.4.4	Start-Up/Shutdown of Server Applications via Command Line	<a href="#"><u>3-20</u></a>
3.4.5	Deinstall AEM-NB from Your System	<a href="#"><u>3-20</u></a>
<b>3.5</b>	<b>Print out Reports</b>	<a href="#"><u>3-21</u></a>

---

# Contents

<b>3.6</b>	<b>Backup and Restore</b>	<a href="#"><u>3-23</u></a>
3.6.1	Basics on Backups and AEM-NB Databases	<a href="#"><u>3-23</u></a>
3.6.2	Commands for Backup, Archive and Restore	<a href="#"><u>3-24</u></a>
3.6.3	Backup, Archive and Restore Procedures	<a href="#"><u>3-26</u></a>
3.6.3.1	Backup Procedure	<a href="#"><u>3-27</u></a>
3.6.3.2	Archive Procedure	<a href="#"><u>3-27</u></a>
3.6.3.3	Restore Procedure	<a href="#"><u>3-27</u></a>
3.6.3.3.1	General	<a href="#"><u>3-27</u></a>
3.6.3.3.2	Full Restoration Procedure	<a href="#"><u>3-27</u></a>
3.6.3.3.3	Incremental Restoration Procedure	<a href="#"><u>3-28</u></a>
3.6.4	Examples for Backup Schedules	<a href="#"><u>3-28</u></a>
3.6.4.1	Daily Cumulative, Weekly Cumulative Backups	<a href="#"><u>3-28</u></a>
3.6.4.2	Daily Cumulative, Weekly Incremental Backups	<a href="#"><u>3-29</u></a>
3.6.4.3	Daily Incremental, Weekly Cumulative Backups	<a href="#"><u>3-30</u></a>
<b>3.7</b>	<b>Log Management</b>	<a href="#"><u>3-31</u></a>
3.7.1	Different Log Types	<a href="#"><u>3-31</u></a>
3.7.2	Configuration of Logs	<a href="#"><u>3-31</u></a>
3.7.3	Log Viewer Window	<a href="#"><u>3-32</u></a>
<b>3.8</b>	<b>Disaster Recovery</b>	<a href="#"><u>3-37</u></a>

## 3.1 Overview

---

This chapter provides you with information about:

- Accessing the *AnyMedia*® Access System Element Manager for Narrow-band Services R1.3 (AEM-NB)
- General handling of the workspace and AEM-NB windows
- Starting up and shutting down applications
- Printing out reports from AEM-NB windows
- Backup and restore tasks
- Basics on log management and how to use the Log Viewer.

## 3.2 System Access

To access the *AnyMedia* Element Manager (AEM-NB) application, you need to have an account in the underlying operating system, and this account has to be accepted as a user account of AEM-NB. The user account has to be NIS (Network Information Name Service) based and the NIS can be provided by the AnyMedia Server or by another machine. AEM-NB user accounts are managed by the administrator (cf. Chapter 4).

### 3.2.1 Login to Operation System

This chapter describes how to log into the system.

**System Login** Complete the following procedure to log in:

Step	Procedure
1.	The system asks for your user name. Enter your user name and press <b>Return</b> or click <b>OK</b> .
2.	The system asks for your password. Enter your password and press <b>Return</b> or click <b>OK</b> .

**Login Correct** If the login was correct, the workspace is displayed.

**Login Incorrect** If the login was incorrect, a warning message appears ("Login incorrect; please try again."). Confirm the message by pressing **Return** or clicking **OK** and repeat the login procedure.

**Start Core Applications** If the core applications were not yet started an administrator has to do this (cf. Chapter 3.4.4, page 3-20) before the AEM-NB access bar can be started.

Before the AEM-NB access bar (cf. Figure 3-1, page 3-3) can be started the setup of the environment must be done with the command

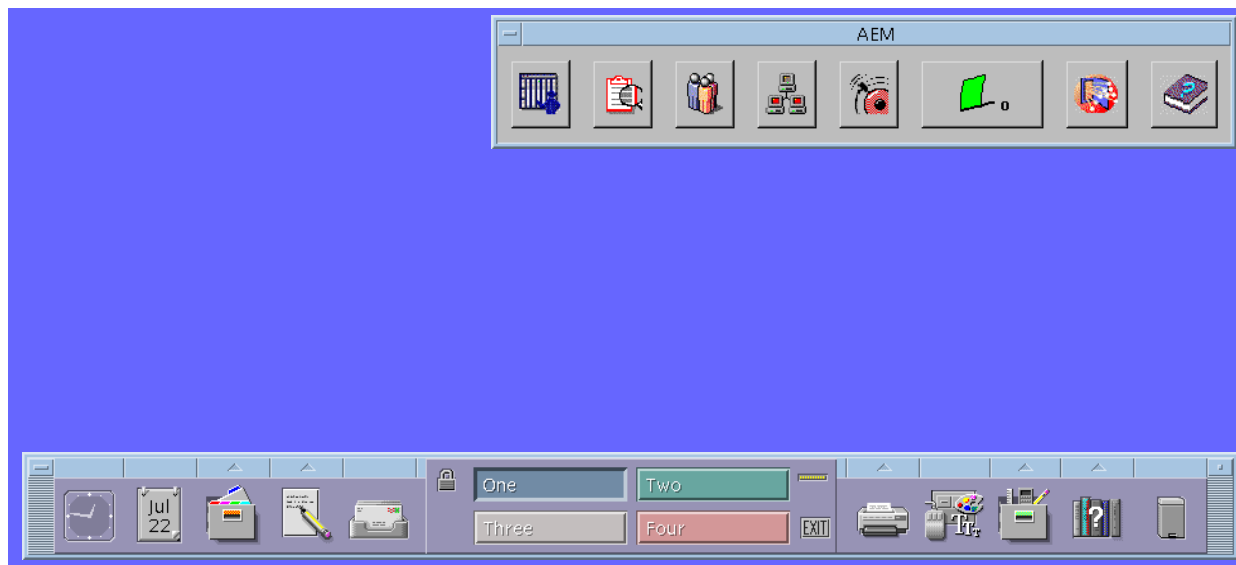
```
. <GUI base path>/GUI/AnyMediaNBEM_GUI.sh
```

The <GUI base path> is the path to the location where the GUI directory is installed on your machine (i.e. /opt/lucent/AnyMediaNBEM\_R1.3). If this command was included in the **.profile** file it needs not to be executed manually.

**Start AEM-NB Access Bar** To start the AEM-NB access bar (cf. Figure 3-1, page 3-3) after a correct login, type in a terminal window, which you can open via the workspace manager (cf. Chapter 3.3.8, page 3-12):

```
cd <GUI base path>/GUI/  
GUI_Main &
```

A splash screen is displayed and then the AEM-NB access bar is shown.



**Figure 3-1** Workspace with AEM-NB Access Bar

### 3.2.2 Logout from Operation System

This chapter describes how to log out from the system. You can log out manually or be logged out automatically after a certain time of mouse and keyboard inactivity.

#### System Logout

Complete the following procedure to log out manually:

Step	Procedure
1.	Close the AEM-NB access bar window.
2.	Click on the <b>Exit</b> symbol in the workspace manager or select <b>Log out...</b> in the workspace menu.
3.	A message box pops up. Press <b>Return</b> or click <b>OK</b> to confirm the logout. Press <b>Cancel</b> not to log out.

After a logout the login screen is displayed again.

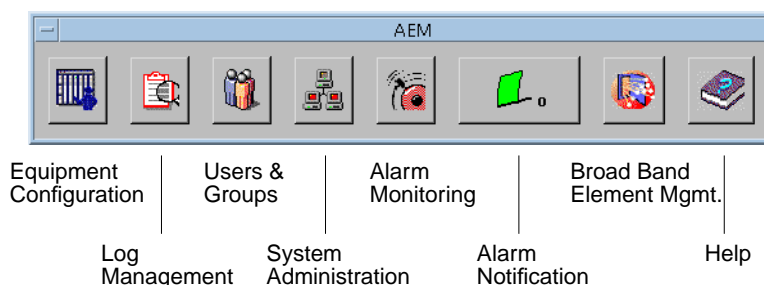


#### NOTE:

During the client installation (cf. 2.2.1.2, page 2-27) a cron process is installed. This cron automatically kills the GUI processes every night due security reason. The execution time of the cron can be changed by the administrator only.

### 3.2.3 AEM-NB Access Bar

The AEM-NB access bar allows access to all AEM-NB applications and offers an alarm indication as well as a help feature.



**Figure 3-2 AEM-NB Access Bar**

**Start Access Bar** To start the access bar see "Start AEM-NB Access Bar" in Chapter 3.2.1.

**Functions** The access bar provides access to the following applications:

- Equipment Configuration (cf. Chapter 5)
- Log Management (cf. Chapter 3.7, page 3-31)
- Users & Groups (cf. Chapter 4)
- System Administration (cf. Chapter 3.4, page 3-17)
- Alarm Monitoring (cf. Chapter 6)
- Alarm Notification (cf. Chapter 3.2.3.1, page 3-4)
- Broad Band Element Management
- Help.

**Start applications** To start an application click on the respective icon.

**Access Control** If an icon of the access bar is grayed, you are not allowed to access this application or the application is not running. Whether access is granted or denied depends on your user group membership. The Alarm Notification and Help icons are always accessible.

#### 3.2.3.1 Alarm Notification Icon

**Description** The Alarm Notification icon displays a flag and a counter. The flag is raised if new alarms are received. The counter is increased every time an alarm is received. By default, only critical alarms affect the Alarm Notification icon. The counting starts with "0" every time the access bar is started. The behavior of the Alarm Notification icon can be changed so that it displays alarms with other severities.

**Reset Counter**

If you click on the Alarm Notification icon, the flag is lowered and the counter re-set.

**Customize Alarm Notification**

The behavior of the Alarm Notification Icon can be customized. It reports only alarms for which the corresponding variable (see Table 3-1) in the system preferences file (`$ANYMEDIAPATH/GUI/cfg/SystemPreferences.ini`) is set to `true`. If the variable is set to `false` it reports no alarms of this alarm severity.

**Table 3-1 Variables for Customizing Visual Alarm Notifications**

Alarm Severity	Variable Name
Critical	VISUAL_CRITICAL_ALARM_SEV
Major	VISUAL_MAJOR_ALARM_SEV
Minor	VISUAL_MINOR_ALARM_SEV
Info	VISUAL_INFO_ALARM_SEV

**Audible Alarm Notification**

If an alarm of a certain alarm severity (default: critical) is received an audible signal is issued. The audible signal is generated only for alarms with an alarm severity for which the corresponding variable (see Table 3-2) in the system preferences file is set to `true`. If it is set to `false` no audible signal is generated for alarms of this alarm severity. Alarms are audible on the server only.

**Table 3-2 Variables for Customizing Audible Alarm Notifications**

Alarm Severity	Variable Name
Critical	AUDI_CRITICAL_ALARM_SEV
Major	AUDI_MAJOR_ALARM_SEV
Minor	AUDI_MINOR_ALARM_SEV
Info	AUDI_INFO_ALARM_SEV

**Make Changes Take Effect**

Changes in the system preferences file take effect only after the next start-up of the AEM-NB GUI clients.

**3.2.3.2 Help Icon****Description**

The Help icon provides access to the AEM-NB online help. If you click on the Help icon the help index is displayed.

**3.2.4 Capacity**

The AEM-NB allows for a maximum of

- 5 simultaneous users
- 100 NEs to be managed.

---

## 3.3 General Information on Keyboard and Windows

---

### 3.3.1 Keyboard

---

The keyboard offers special keys which are pressed individually or in combination with others to perform specific actions.

#### Special Keys

The most important special keys are:

- **Return**, to confirm an entry or to start a new line when a text consisting of several lines is entered
- **Esc** = "Escape" to initiate an escape sequence, i.e. the keys pressed after pressing Esc are interpreted as an instruction and not as entered text
- **Ctrl** = "Control" to initiate a control sequence. **Ctrl** is always used in combination with one or several other keys and represents an instruction
- **Alt** = "Alternate" is pressed in combination with one or more other keys thereby assigning these keys another meaning
- **Backspace** or **Del** (= "Delete") to delete all characters to the left of the cursor.

#### Conventions

The keys on the keyboard are represented in the text in the following way: **Ctrl**, **Backspace**, **A**, **B**,...

Two or more of these keys connected by a hyphen ("-") indicate that they must be pressed simultaneously. **Shift-Ctrl-A**, for example, means that the "A" key must be typed while holding down **Shift** and **Ctrl**.

Keys that are separated by blanks only must be pressed one after the other. **Esc A B**, for example, means that **Esc** must be pressed first followed by **A** and then **B**.

### 3.3.2 Mouse

---

#### Conventions

When using the mouse, you will frequently find the following terms:

- **Click** or **Select**: Position the cursor on an object and press the left mouse button.
- **Double click**: Click the left mouse button twice in rapid succession.
- **Drag**: Move the mouse keeping the left mouse button pressed.



### 3.3.3 Different Aspects of the Cursor

---

The aspect of the cursor will vary to indicate the actions you may currently undertake using the mouse.

The following symbols show examples for possible cursor aspects:



The arrow up pointing to the left is used to select objects and to press buttons.



The "I" beam is used within a text field to indicate the position where text is to be inserted.



The "clock" cursor indicates that in the window where the cursor is positioned a process requiring a lot of processing time is running and no mouse or keyboard inputs are possible.

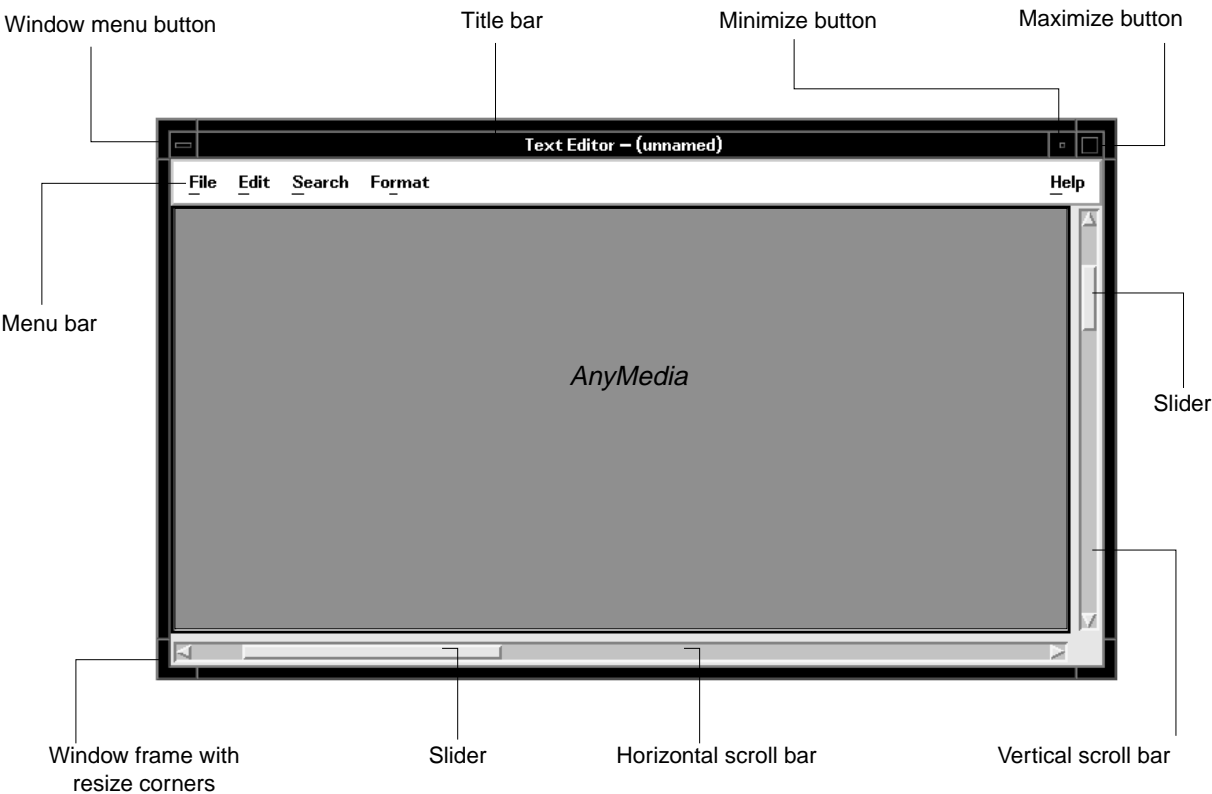
### 3.3.4 Basics on Windows

---

The window which contains the **input focus** evaluates all keyboard and mouse inputs. The window containing the input focus is easy to distinguish from other windows opened on the screen by the different colour of its window frame.

Use the mouse to direct the input focus to a defined window. Click on a position within the window or place the cursor on the window.

The window shown in Figure 3-3 labels the different window controls which allow the user to change the aspect of the window on the screen and the process represented by the window.



**Figure 3-3 Specimen Window and Window Controls**

The individual window controls shown in Figure 3-3 are:

**Figure 3-4 Controls in a Window**

Window Part	Function
Window frame with resize corners	The frame delimits the window on the screen and its colour indicates whether this window contains the input focus. Drag the frame to shift and resize the window. By dragging the window corners, the window size may be modified to both limiting sides at the same time.
Title bar	The title bar informs you about the function of the window. Drag the title bar to shift the window on the screen.
Minimize button	If you click on the minimize button, the window will be displayed in its minimum size, i.e. it will appear as an icon on the screen, though the process represented by the window will continue running.

**Figure 3-4 Controls in a Window**

Window Part	Function
Horizontal scroll bar	<p>Use the horizontal scroll bar and the slider to shift the visible window section to the left or right.</p> <ul style="list-style-type: none"><li>■ Small step to the left or right: Click on the left or right scroll bar arrow.</li><li>■ Page left or right: Click on the scroll bar to the left or right of the slider.</li><li>■ Shift window section: Use the mouse and drag the slider horizontally until the desired window section becomes visible.</li></ul>
Vertical scroll bar	<p>Use the vertical scroll bar to shift the currently visible window section up or down:</p> <ul style="list-style-type: none"><li>■ Small step up or down: Click on the top or bottom scroll bar arrow.</li><li>■ Page up or down: Click on the scroll bar section above or below the slider.</li><li>■ Shift window section: Use the mouse and drag the slider up or down until the desired window section becomes visible.</li></ul>
Maximize button	<p>Activate the maximize button by clicking on it to show the window at its maximum size, i.e. the window will occupy the whole screen. If you click again on the maximize button thus activated, the window will be restored to its original size.</p>
Menu bar	<p>The menu bar contains the menu names, each of them containing options related to the topic. These options may be selected to control the process running in this window (cf. Chapter 3.3.6)</p>
Window menu button	<p>Click this button to open the window menu (cf. Figure 3-5). Double click to exit the application.</p>

### 3.3.5 Window Menu

A window can be provided with a window menu. The window menu allows to alter the appearance of the window or to exit the application represented by the window.



**Figure 3-5 Window Menu**

To open the window menu shown in Figure 3-5, click on the window menu button or click with the right mouse button on the window frame.

The menu options in the window menu are listed in the following table.

**Table 3-3 Window Menu Items and their Function**

Menu Item	Function
<b>Restore</b>	A window currently being represented as an icon or in its maximum size is restored to its original size.
<b>Move</b>	Allows you to move the window interactively on the screen. The window frame will follow the mouse movements until you press the left mouse button.
<b>Size</b>	Allows interactive resizing of the window. Move the cursor appearing in the window to the window edge you wish to move. The edge will follow the mouse movements until you press the left mouse button.
<b>Minimize</b>	The window is shown as an icon.
<b>Maximize</b>	The window is shown in its maximum possible screen size.
<b>Lower</b>	If there are several overlapping windows, the currently active window is shifted to the bottom of the pile.
<b>Close</b>	This function will close the window and remove it from the user interface, exiting the application linked to the window.

### 3.3.6 Menu Bar

**Menu Options** The menu bar of a window contains the menu names. Once you click on a menu it opens and a series of related menu options will be displayed under the menu name.

**Conventions** Each option represents a function, which can be used to control the application running in the window. To call this function, click on the required option. A menu option is referred to in the text as: "**Menu name -> Menu option**" (e.g. in the menu below: **Network View -> Maps**).

A grayed menu name or option cannot be selected.

**Submenu Conventions** Submenus are menus opening under a certain menu option and containing a number of related menu options. Some menu options are provided with a small arrow pointing to the right (>). These menu options have a submenu that will open as soon as you click on the menu option. A submenu option is referred to in the text as "**Menu name -> Menu option -> Submenu option**" (e.g. "**Network View -> Submaps -> Open/List...**"). A submenu option again may offer a submenu, then an appropriate number of "->" is added.

### 3.3.7 Cursor Menu

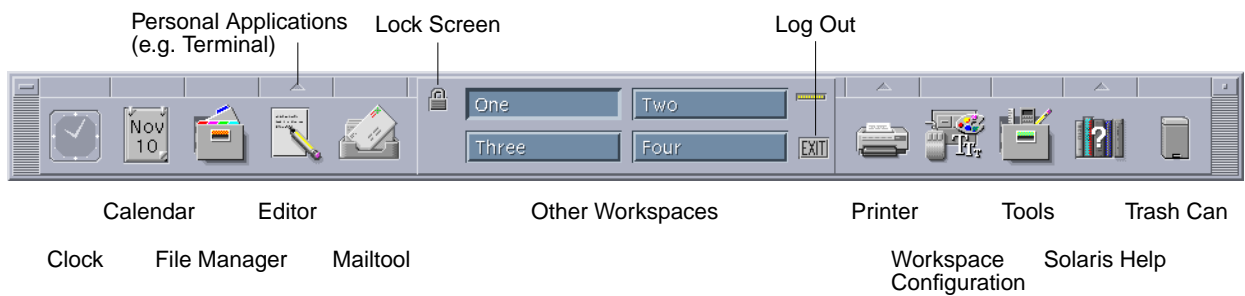
**Menu at the Cursor Position** Some objects in windows have a menu associated with them. This menu will pop up at the cursor position when the right mouse button is pressed. The cursor must not, however, be positioned on a menu bar or a window frame. The cursor menu is not available in all windows. The functions which can be executed using this cursor menu depend on the application of the respective window.

**Select Menu Option** Proceed as follows to select a menu option from the cursor menu:

Step	Procedure
1.	Press the right mouse button.
2.	Move the cursor onto the desired menu option.
3.	Click the left or right mouse button to execute the menu option, or if you do not wish to execute a menu option, move the cursor away from the menu and click somewhere outside the menu.

3.3.8      **Workspace Manager**

**General**                      After logging in to the operation system (SUN Solaris), the workspace manager window is situated at the bottom of the screen offering a range of functions and information. A function is initiated by clicking the respective area of the workspace manager. In Figure 3-6 only an example of the workspace manager is given, as the entries are configurable.

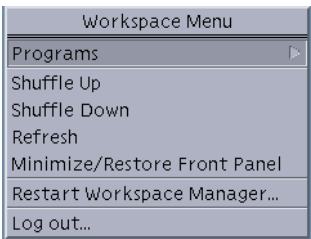


**Figure 3-6      Workspace Manager**

**Functions**                      For a detailed description of the offered functions, please refer to your *Solaris User's Guide* and *Solaris Common Desktop Environment User's Guide*.

3.3.9      **Workspace Menu**

**General**                      The workspace menu opens when you click with the right mouse button on the background of the workspace.



**Figure 3-7      Workspace Menu**

**Workspace Menu Functions**

The workspace menu provides the functions listed in the following table:

**Table 3-4 Menu Items of the Workspace Menu**

Menu Item	Function
Programs	A submenu offering several programs.
Shuffle Up	If several windows on the screen are layered on top of one another, "Shuffle Up" brings the window from the very bottom to the top of the pile.
Shuffle Down	If several windows on the screen are layered on top of one another, "Shuffle Down" moves the window from the top of the pile to the very bottom.
Refresh	The contents of the windows on the screen and the screen backdrop are refreshed.
Minimize/Restore Front Panel	The workspace manager window is reduced to an icon or, if already iconized, restored to a window.
Restart Workspace Manager...	The workspace manager is restarted. Some of the changes to the user interface become valid only after the restart of the workspace manager. The restart must be acknowledged in a window.
Log out...	A logout from the system can be initiated.

### 3.3.10 Controls in AEM-NB Windows

**Introduction**

The windows of the AEM-NB display certain controls (buttons, text fields, etc.). These controls are the same in all AEM-NB windows and explained in this chapter.

**Grayed Controls**

All controls within a window can be activated by clicking on them only if they are not grayed.

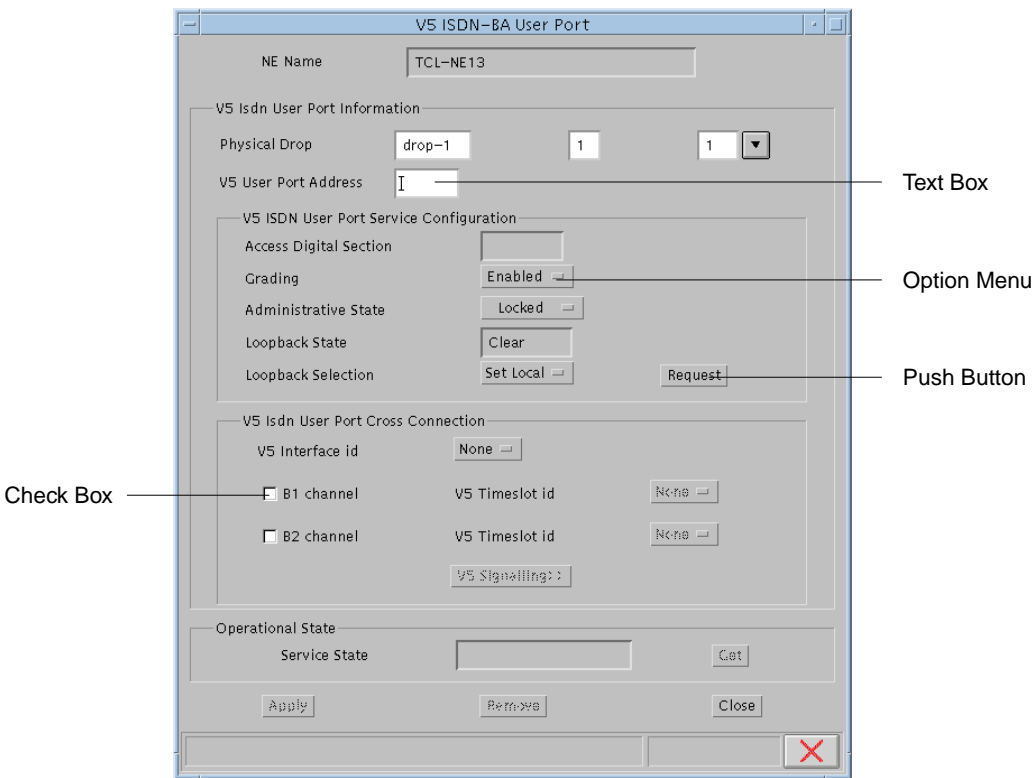


Figure 3-8 Example of an AEM-NB Window

**Convention** The following font is used when a button is mentioned, e.g. **Close**.

The following elements are used within windows:

- **Push Button**  
Each push button is provided with a designation describing its function. If you click on the push button, the function will be executed. If you click on a push button, the designation of which is followed by three dots (e.g.: **Help...**), a window will open where you may set further parameters. Push buttons which alter their designation depending on context are also called **Label buttons**.
- **Check Box**  
Check boxes have the same function as an on/off switch. Each time you click on a check box, you will change its toggle status. A (pressed) check box containing a check mark means that the option at this position is selected.



- Radio Button

Radio buttons have the same function as check boxes, with the difference that of various radio buttons of the same group, only one can be pressed at a time. As with a radio set, a set button will pop out when you press the next one in.

- Text Box

Text boxes are used to input text via the keyboard.

- List Box

A list box contains read-only data in list form. To scroll through a list you have to use the scroll bar at the right of the list box. If the list box allows the selection of entries, more than one entry can be selected by clicking on all desired entries once while the **Ctrl** key is pressed. If more entries are selected you can deselect a certain one by clicking on it again, while the **Ctrl** key is pressed. A range of consecutive entries can be selected simultaneously by clicking on the first entry of the range and then on the last while the **Shift** key is pressed.

- Drop-Down List Box

A drop-down list box allows you to enter data by selecting an entry from a list that drops down after clicking on the triangle on the right of the box.

- Spin Box

A spin box only allows a limited set of discrete ordered input values. You have to use the up and down arrows to increment or decrement the value.

- Tab

A window can contain a register of several tabs. Clicking on a tab displays the corresponding contents in the window.

- Option Menu

The option menu is used to set a certain option. Its designation will indicate the option currently set. Handling of the option menu is the same as for a menu.

## Frequently Used Buttons

The table below provides an overview of buttons which have the same function in every AEM-NB window:

**Table 3-5 Function of Frequently Used Buttons**

Button	Function
<b>OK</b>	Applies changes; window is closed
<b>Apply</b>	Applies changes; window stays open for further edits
<b>Cancel</b>	Discards changes; running operation is cancelled; window is closed
<b>Close</b>	Discards changes; window is closed

**Frequently Used Menus**

The table below provides an overview of menus which have the same function in every AEM-NB window:

**Table 3-6 Function of Frequently Used Menus**

Menu	Function
<b><i>File -&gt; Print -&gt; Print Table</i></b>	Prints the contents of text lists in the window (cf. Chapter 3.5, page 3-21). Opens the Print Dialog window to set parameters for the print out.
<b><i>File -&gt; Print -&gt; Print Window</i></b>	Prints a screenshot of the whole window (cf. Chapter 3.5, page 3-21). Opens the Print Dialog window to set parameters for the print out.
<b><i>File -&gt; Print -&gt; Preview</i></b>	Shows how it will be printed if the "Print Table" option is used. Opens directly the Print Preview window.
<b><i>File -&gt; Exit</i></b>	Closes all windows of this application.
<b><i>Help -&gt; On Window</i></b>	Displays online help for this window.
<b><i>Help -&gt; Index</i></b>	Displays online help index.

## 3.4 Application Start-Up and Shutdown

### 3.4.1 General on Applications

#### Definitions

The following tables gives definitions of terms used in this chapter.

**Table 3-7 Definitions for Applications**

Term	Meaning
Server application	Set of server processes that perform a certain functionality. Server applications provide services for client applications.
Client application	Set of processes that use the services provided by the server applications (e.g. GUI and Northbound users)
Level 1 or core applications	The minimum set of server applications that have to run together to provide the minimum functionality of the AEM-NB. These applications must run to allow the Level 2 Application to be started up. These applications are shown as only one running application. If this group is shut down the AEM-NB is shut down.
Level 2 applications	The server applications that can be started-up and shut-down individually without affecting the functioning of other applications. However, there are interdependencies between Level 2 applications so that the shut-down of one may affect the services of others.

There are three ways to start the server applications:

- at boot time

Root can configure the system at the installation so that Level 1 applications only or Level 1 and all Level 2 applications start at boot time.

- via command line

The administrator can start Level 1 applications or Level 1 and all Level 2 applications via command line.

- via GUI

The administrator can start any desired Level 2 application from the GUI once Level 1 is already running.

### 3.4.2 AEM-NB Server Applications

---

The AEM-NB consists of four server applications. The following list gives their names and uses:

- **System core**  
Provides basic functionalities and is needed by all applications. If this server application is shut-down, all other applications are shut down and all client applications are notified of the shutdown.
- **Configuration management**  
needed by the configuration management application (cf. Chapter 5). If this server application is shut down, the configuration management application will no longer run.
- **Alarm management**  
needed by the fault/alarm management application (cf. Chapter 6). If this server application is shut down, the fault/alarm management application will no longer run.
- **Network element management**  
Needed for operations which affect NEs. If this server application is shut down, operations with NEs can no longer be carried out. All client applications continue working, except for those parts involving NEs.

#### **Restart of Server Applications**

If a server application crashes, the AEM-NB tries to start-up this server application one time automatically. If the server application start-up mechanism fails, and it is a level 2 application, it remains stopped. If it is a level 1 application, the whole system is shutted-down and restarted (all running applications at that moment are shutted-down and restarted).

### 3.4.3 Start-Up/Shutdown of Server Applications via GUI

---

#### **Introduction**

The System Administration function of the access bar allows to start up or shut down server applications manually and to monitor the state of each application. Only the administrator has access to this function. The "System Administration" window is shown below.

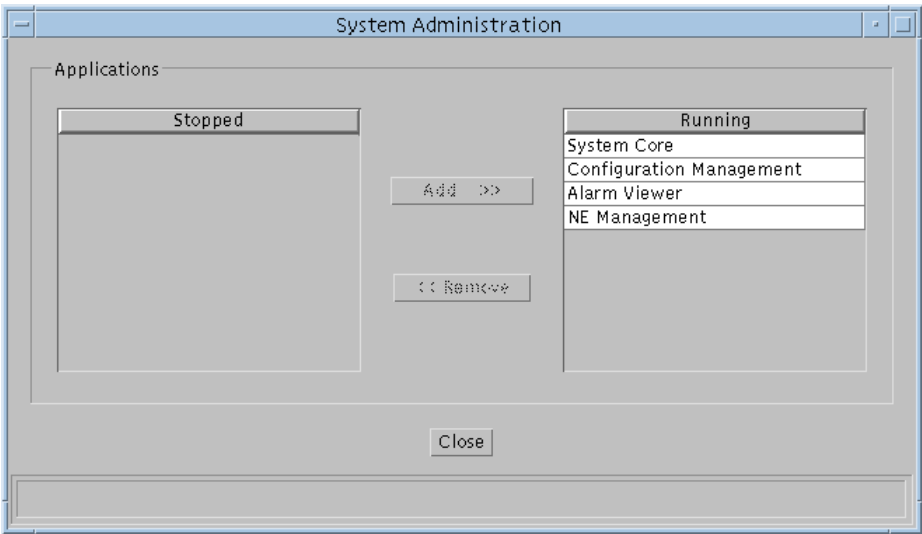


Figure 3-9 System Administration

Stopped/Running Lists

The "System Administration" window displays two lists: **Stopped** and **Running**. The **Stopped** list contains all applications which are not running. The **Running** list contains all running applications. You can stop running or start stopped applications.

The following table provides an overview of the possible actions in the "System Administration" window.

Table 3-8 System Administration Actions

If you want to...	then...
start one or more applications	select the applications which shall be started under <b>Stopped</b> and press <b>Add</b> .
shut-down one or more applications	select the applications to be shut down under <b>Running</b> and press <b>Remove</b> .
close the window	press <b>Close</b> or select <b>File -&gt; Exit</b> .

Start/Shut-down more applications

You may start or shut-down more than one application at the same time. To do so, click on all desired applications once while the **Ctrl** key is pressed. If more applications are selected you can deselect a certain application by clicking on it again, while the **Ctrl** key is pressed. A range of consecutive lines can be selected simultaneously by clicking on the first line of the range and then clicking on the last line while the **Shift** key is pressed.

### 3.4.4 Start-Up/Shutdown of Server Applications via Command Line

The system can be configured at installation time to start-up the server applications automatically on every reboot. An administrator can start-up or shut-down server applications via a command line interface.

#### Commands for Start-Up and Shut-Down

The following table shows which commands have to be entered in a terminal window to start-up or shut-down server applications.

**Table 3-9 Commands for Start-up and Shut-down**

If you want to...	type in a terminal window...
start-up all AEM-NB applications	<code>SystemAdmin ALL</code>
start-up the core AEM-NB applications	<code>SystemAdmin CORE</code>
shut-down all AEM-NB applications	<code>SystemAdmin CLEAN</code>

### 3.4.5 Deinstall AEM-NB from Your System

#### De-Installation

The AEM-NB software can be deinstalled from your system. The de-installation removes all AEM-NB related items (databases, 3rd party software, etc.), which have been installed at the time when AEM-NB was installed, from your system.

#### Commands for De-Installation

The following table shows which commands have to be entered in a terminal window to de-install AEM-NB from your system. Log in as root to execute these commands:

**Table 3-10 Commands for De-Installation**

If you want to...	type in a terminal window...
remove the server package	<code>pkgrm LuANY10S</code>
remove the client package	<code>pkgrm LuANY10C</code>
remove third-party software	<code>pkgrm LuRWRT</code>

For details about the above commands, please refer to Chapter 2.2.4.1 Remove AnyMedia Servers package, Chapter 2.2.4.2 Remove AnyMedia Client package and Chapter 2.2.4.3 Remove Third-Party packages.

## 3.5 Print out Reports

### General

The "Print Dialog" (cf. Figure 3-10) is used from any application within AEM-NB to generate an output of data. It pops up when you press **Print Table** or **Print Window** in a window or **Print** in the Print Preview window. When you choose **Print Preview** in a window the Print Preview window (cf. Figure 3-11, page 3-22) pops up.

### System Details for Printing

If the Unix command "lp" does not exist or is not configured on your system the AEM-NB software will not be able to print. This is because the print-out is first converted to PostScript format and then piped to the Unix command "lp -d printer\_name" where **printer\_name** is replaced by the value entered in the **Printer** field of the "Print Dialog".

Figure 3-10 shows an example of the "Print Dialog".

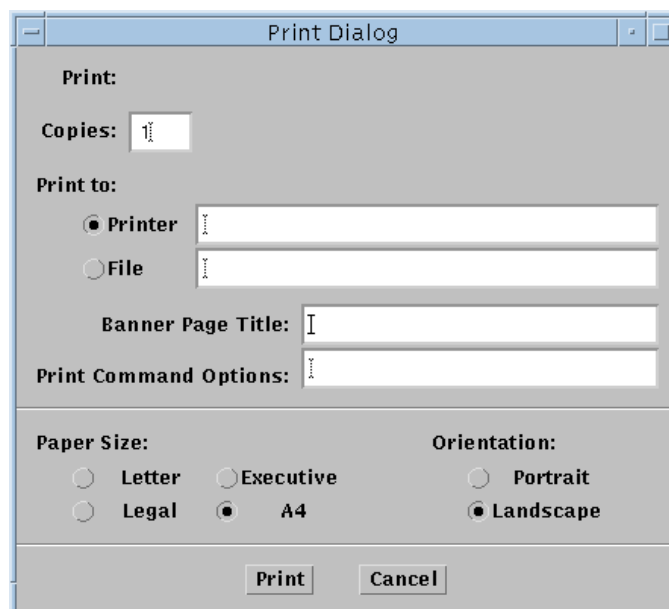


Figure 3-10 Print Dialog

### Actions in Print Dialog

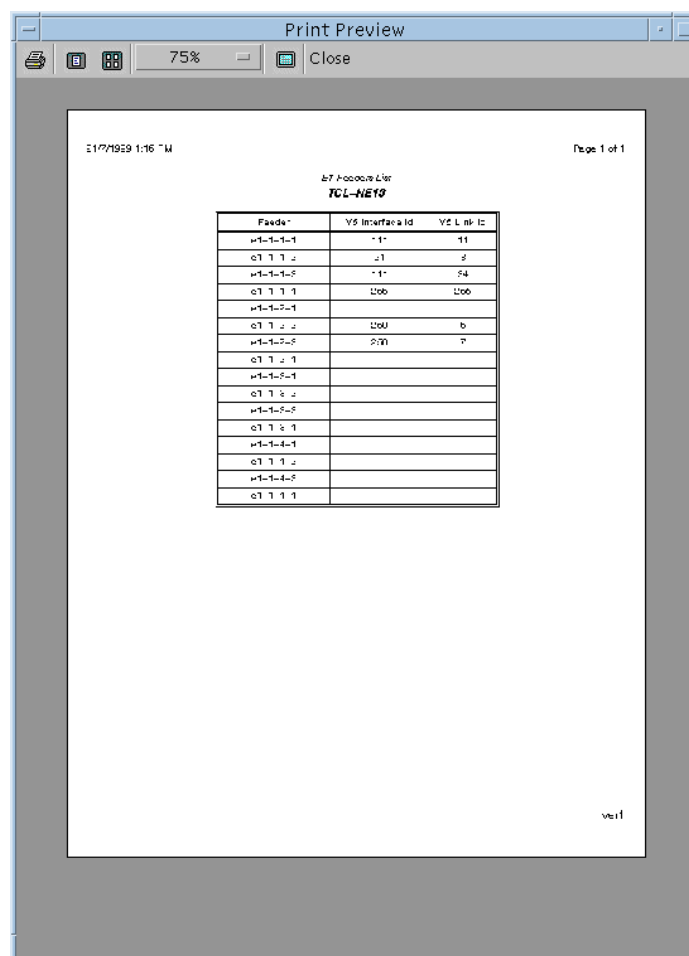
The following table provides an overview of the possible actions in the "Print Dialog".

Table 3-11 Print Dialog Actions

If you want to...	then...
print multiple copies	enter the number of copies in <b>Copies</b> .
print to a printer	enter the name of the printer in <b>Printer</b> .
print to a file	enter the name of the file in <b>File</b> .

**Table 3-11 Print Dialog Actions**

If you want to...	then...
have a title over the printed pages	enter the title in <b>Banner Page Title</b> .
apply UNIX print options	enter the options in <b>Print Command Options</b> .
select the paper size	click one of the radio buttons below <b>Paper Size</b> .
select the orientation of the print out	click one of the radio buttons below <b>Orientation</b> .
start printing and close the window	click on <b>Print</b> .
close the print window without printing	click on <b>Cancel</b> .

**Figure 3-11 Print Preview Window**



**Actions in Print Preview**

The following table provides an overview of the possible actions in the "Print Preview".

**Table 3-12 Print Dialog Actions**

If you want to...	then...
print out	click on the <i>printer icon</i>
cancel the print out	click on <i>Close</i>
view a single page preview	click on the <i>single page icon</i>
view a multi page preview	click on the <i>multi page icon</i>
change the magnification of the preview	select another magnification with the <i>% option menu</i>
maximize/restore the preview window	click on the <i>monitor icon</i>

## 3.6 Backup and Restore

The backup functions of the AEM-NB allow you to copy AEM-NB related file systems to removable media (such as tape) to safeguard against loss, damage, or corruption. The AEM-NB system files and database backup allows to back up and restore system files and databases belonging to the installed applications (e.g. configuration files). Archiving is possible for AEM-NB log files.

The restore functions allow you to restore file systems by copying reasonably current backup files from removable media to a working directory.

### 3.6.1 Basics on Backups and AEM-NB Databases

**Definitions**

The following table gives definitions of terms used in this chapter.

**Table 3-13 Definitions**

Term	Meaning
Backup	process of copying file systems to removable media (such as tape) to safeguard against loss, damage, or corruption.
Archive	process of copying file systems to removable media (such as tape) and deleting the original files once they have been backed up.
Restore	process of copying backup files from removable media to a working directory, replacing the original files which could have been damaged.
Full Backup	copies a complete file system or directory

**Table 3-13 Definitions**

Term	Meaning
Incremental Backup	copies new files and files that have changed since a previous backup. The incremental backups are usually given a dump level which determines which files are backed up. A certain level incremental backup will save all the new or changed files since the last backup with a lower level.
On-line Backup	backups performed on user demand
Off-line Backup	backups performed automatically via any scheduling mechanisms, e.g. cron file

**Backup Types**

There are three different backup types. The following list shows their differences and advantages:

- Full backup

A full backup copies a complete file system or directory, e.g. all AEM-NB data. This method requires large numbers of backup tapes that take a long time to write and takes also some time to retrieve individual files because the backup drive has to move sequentially to the point on the tape where the file is located. On the other hand, using full backup makes it easier to retrieve small changes in file systems.

- Incremental backup

An incremental backup only includes copies of new files and files that have changed since a previous backup. It is available for database files only. Requires less resources, but searching for a certain file on the incremental tapes can take time.

### 3.6.2 Commands for Backup, Archive and Restore

#### Default Locations of Data for Backups or Archives

If a backup is done, the four AEM-NB databases, the NVDS and the log files are copied to the backup medium. If an archive is made the log files are moved to the backup medium. The files from which a backup or archive is done are shown in the table below. The location of the files is relative to the main installation directory. (For changing default locations refer to Appendix B.)

**Table 3-14 Default File Names for Backup and Archive**

Database/File	File Name (Directory/File)	Backup Fails if File doesn't exist
Alarm database	AM/db	yes
Configuration management database	CM/db	yes
NE management database	NEM/db	yes

**Table 3-14 Default File Names for Backup and Archive**

Database/File	File Name (Directory/File)	Backup Fails if File doesn't exist
Security database	Security/db	yes
Non-volatile Data Storage (NVDS)	CM/nefiles/NVDS	no
Log Files	log (directory)	no

**System Message**

After each backup, archive or restore command a result message is displayed, which indicates whether the operation was successful or not. This message is displayed only if the command was entered on the command line.

**Command Syntax**

In the following description of the commands, square brackets, e.g. [-c], indicate optional parameters. The pipe symbol "|" indicates alternative options from which one has to be chosen, e.g. **INC|FULL**. All parameters not enclosed in brackets are mandatory. Each command is entered without enclosing parameters in brackets.

**Backup Files**

Use the following command to make a backup of a database or directory. If you enter none of the optional parameters, a backup of all data necessary to restore the AEM-NB will be done:

```
AEMNB_backup [-h|-H] [-c] [-p path] [-f file] [-t INC|FULL] [-l level]
```

Parameter description:

- h, -H** Display command syntax (**-h**) or additional help (**-H**).
- c** Aborts a running backup operation.
- p *path*** *path* is the directory or device to back up. (Default: value of the variable **OAM.backup.backupDirectory**, which is set in the file **AnyMediaNBEM.cfg**.)
- f *file*** Location of the backup file. *file* can be a local file or a locally mounted file (in case a local tape device is used *file* specifies a "soft label"). (Default file names:  
EM\_SYSBCK\_yyyymmdd.fullbck for full backup  
EM\_SYSBCK\_yyyymmdd.incbck for incremental backup,  
with yyyy = year, mm = month, dd = day of the backup.)
- t **INC|FULL**** Type of backup: incremental (**INC**) or full (**FULL**). (Default: **FULL**). This parameter is ignored if "**-l 0**" is used.
- l *level*** Specifies the backup level. Files modified since last backup at a lower level are copied, *level* = 0...9. This parameter is ignored if "**-t FULL**" is used.

**Restore Files**

Use the following command to restore a database or directory:

```
AEMNB_restore [-h|-H] [-c] [-p path] -f file
```

Parameter description:

- h, -H** Display command syntax (**-h**) or additional help (**-H**).
- c** Aborts a running restore operation.
- p path** **path** is the directory or device to which the restored data should be written. (Default: value of the variable **OAM.backup.backupDirectory**, which is set in the file **AnyMediaNBEM.cfg**.)
- f file** Location of the backup file. **file** can be a local file, a locally mounted file or a local tape device.

**Archive Files**

Use the following command to archive log files. This function is primarily intended to archive the AEM-NB log files. If you enter none of the optional parameters, the AEM-NB log files will be archived.

```
AEMNB_archive [-h|-H] [-c] [-p path] [-f file]
```

Parameter description:

- h, -H** Display command syntax (**-h**) or additional help (**-H**).
- c** Aborts a running archive operation.
- p path** **path** is the directory or device to archive. (Default: value of the variable **OAM.backup.backupDirectory**, which is set in the file **AnyMediaNBEM.cfg**.)
- f file** Location of the backup file. **file** can be a local file or a locally mounted file (in case of a local tape device is used **file** specifies a "soft label"). (Default file name: **EM\_SYSARCH\_yyyymmdd.arc**, with yyyy = year, mm = month, dd = day of the archive.)

### 3.6.3 Backup, Archive and Restore Procedures

---

This section gives an overview of the steps necessary for a backup, archive or restore operation.

**Prerequisite for Backup, Restore and Archive**

The backup, archive or restore commands require that some path system variables are properly set. This is done by the command **AnyMediaNBEM.sh** during the installation of AEM-NB. If this command was not executed the backup, archive or restore commands will not work.

**Different Users**

When different users perform backup, archive or restore operations the system will display a message asking whether temporary data which remained from the previous user should be deleted. If such a message is displayed you must confirm the deletion of these data.

### 3.6.3.1 Backup Procedure

The backup operation needs no user interaction after the backup command was executed.

### 3.6.3.2 Archive Procedure

The archive operation needs no user interaction after the archive command was executed.

### 3.6.3.3 Restore Procedure

#### 3.6.3.3.1 General

##### Default Locations for Restored Data

When a backup is restored, all files are restored to their original location. When archives are restored they are copied into the directory **restored** (relative to the main installation directory).

##### Restore One of Several Backups from Tape

When more than one backup is placed on a tape and a particular one shall be restored, the name of this backup must be known and the tape must be positioned at the beginning of this backup. The name can be determined by using the **tar** command. For example: **tar tvf /dev/rmt/0mn**. The positioning is done as described below.

##### Position Tape

If you know the order of the backups on tape, you can position the tape at the beginning of the desired backup as follows: Rewind the tape (e.g with **mt -f /dev/rmt/0m rewind**) and issue a **tar** command (see example above) until the backup which comes before the one which shall be restored is displayed. If you do not know the order of the backups on the tape, it can be determined as follows: Rewind the tape and then repeatedly issue a **tar** command (see example above) until the backup to be restored is displayed while you note the order of the backups on tape. Then you can position the tape as shown above.

#### 3.6.3.3.2 Full Restoration Procedure

When the restore command is executed the user must decide which image type should be restored. The restore script displays the following message:

Please enter the type of the image to be restored [backup/archive]

Type **backup** or **archive** and press **Enter**.

##### Copy of Originals

Copies of the original databases are saved to allow for a cancellation of the operation. If such a copy could not be made the appropriate image can nevertheless be restored, but a warning is issued. For each database for which no copy could be made the following message is displayed:

Actual <DATABASE TYPE> is not present or ObjectStore copy operation failed.  
The AnyMedia NB-EM system state cannot be recovered if a cancellation is requested.  
Do you want to continue? [y/n]

Type **y** and press **Enter** to continue with the restore procedure. If you type **n** the restore command stops with an error message, no data are restored and the sys-

tem will not work unless a correct restore is performed. When the original databases are present, the message above is not displayed.

### **Additional Incremental Backups**

While the different databases are restored certain information is displayed on the screen. Then the restoration tool asks whether additional databases should be restored:

Do you wish to restore from any additional incremental backups? (yes/no):

Type **no** and press **Enter**.

After that the execution of the restore tool finishes and the restoration is complete.

### **3.6.3.3 Incremental Restoration Procedure**

Before a certain incremental backup can be restored the previous full backups and possibly some previous incremental backups must be restored.

The procedure to restore an incremental backup is the same as the above described procedure for a full backup except for the last ("Additional Incremental Backups") step. In that step the restore tool asks for a confirmation that all needed full backups which are a prerequisite for the incremental backup are present. Answer this question affirmatively. After that the execution of the restore tool finishes and the restoration is complete.

## **3.6.4 Examples for Backup Schedules**

### **Introduction**

This section gives you some examples for typical backup schedules and explains the backup level.

### **Backup Level**

Crucial for the understanding of the backup schedules is understanding the backup level. The backup level is a number which is assigned by you to every backup you make. Each time you make a new backup only those files are put on the back-up media which were altered since the last backup with a lower backup level. A backup level "0" means a full backup.

### **3.6.4.1 Daily Cumulative, Weekly Cumulative Backups**

This is the most commonly used backup schedule. It is recommended for most situations.

### **Schedule Characteristics**

This schedule has the following characteristics:

- Each weekday backup accumulates all files changed since the end of the previous week (or the initial level 0 backup).
- Each Friday's backup contains all files changed since the first level 0 backup. For the level 9 backups, the previous level 0 or level 5 is the closest backup at a lower level.
- Each Friday's backup contains all files changed during the month to that point.

**Example**

The following table shows the backup levels for each days backup. Once a month, a backup with backup level 0 must be performed.

**Table 3-15 Backup Levels of Each Backup**

	variable	Mon	Tue	Wed	Thu	Fri
1st of month	0					
1st week		9	9	9	9	5
2nd week		9	9	9	9	5
3rd week		9	9	9	9	5
4th week		9	9	9	9	5

The following table shows how files accumulate in the backup for each weekday.

**Table 3-16 Example for Files in Backup for Two Weeks**

	Mon	Tue	Wed	Thu	Fri
1st week	ab	abc	abcd	abcde	abcdef
2nd week	g	gh	ghi	ghij	abcdefghijk

### 3.6.4.2 Daily Cumulative, Weekly Incremental Backups

**Example**

The following table shows the backup levels for each days backup. Once a month, a backup with backup level 0 must be performed.

**Table 3-17 Backup Levels of Each Backup**

	variable	Mon	Tue	Wed	Thu	Fri
1st of month	0					
1st week		9	9	9	9	3
2nd week		9	9	9	9	4
3rd week		9	9	9	9	5
4th week		9	9	9	9	6

The following table shows how files accumulate in the backup for each weekday.

**Table 3-18 Example for Files in Backup for Two Weeks**

	Mon	Tue	Wed	Thu	Fri
1st week	ab	abc	abcd	abcde	abcdef
2nd week	g	gh	ghi	ghij	ghijk

### 3.6.4.3 Daily Incremental, Weekly Cumulative Backups

#### Example

The following table shows the backup levels for each days backup. Once a month a backup with backup level 0 must be done.

**Table 3-19 Backup Levels of Each Backup**

	variable	Mon	Tue	Wed	Thu	Fri
1st of month	0					
1st week		3	4	5	6	2
2nd week		3	4	5	6	2
3rd week		3	4	5	6	2
4th week		3	4	5	6	2

The following table shows how files accumulate in the backup for each weekday.

**Table 3-20 Examples for Files in Backup for Two Weeks**

	Mon	Tue	Wed	Thu	Fri
1st week	ab	cd	ef	h	abcdefghi
2nd week	jk	lmn	o	p	jklmnopqr



## 3.7 Log Management

The log management records information on events in the AEM-NB. The logged events can be viewed with the Log Viewer.

### 3.7.1 Different Log Types

There are three log types within the Log Viewer:

- Actions

It contains all the information on actions performed by users or the AEM-NB and which imply changes in the AEM-NB configuration, equipment (NE) configuration, service and subscriber configuration, access to the AEM-NB, print reports and backup& restore. That means all operations triggered by the user or the AEM-NB and all subsequent actions. Also the results of operations are logged in the actions log.

- System Internal Events

It contains all internal events or actions which report unusual changes in the configuration and state of the AEM-NB or indicate errors which occurred in the AEM-NB.

- Autonomous Reports

It contains all information valuable for the equipment supplier about alarms (NE and platform), the performance and all TL1 messages sent from the NE which imply changes in the AEM-NB database.

### 3.7.2 Configuration of Logs

#### Log size

The following values can be configured (conf. Appendix B) for the log system by the administrator:

- Minimum number of days (incl. current day) in the log (default: 7 days)
- Maximum size of all logged data (default: 15 Mbyte).

#### Log Grows Too Big

The logs are stored as separate files, one file holds one day of one log type. If the size of the logged data has reached the size limit and a new event to be logged occurs, some of the already logged data has to be deleted. The oldest recorded

day of one of the logs holding the largest number of days is always deleted. The log system determines which log shall be shortened as follows:

**Table 3-21 How the Log be Shortened is Determined**

If...	then the log system will...
only one log type holds more days than the others	delete oldest recorded day of this log type.
the longest log types hold the same number of days and the log for which an event shall be logged is among these logs	delete oldest recorded day of the log type for which an event shall be logged.
the longest logs hold the same number of days and the log for which an event shall be logged is not among these logs	select one of the longest log types in the following order: Autonomous Report, Actions, System Internal Events and delete oldest recorded day of this log type.

### Alarms

The log system issues an alarm if

- one of the logs is shortened to a number of days below the minimum number of days. (I.e. also, if a log is shortened that already holds fewer than the minimum number of days.) Alarm name: LOG\_DEL\_PART.
- the current day of a log is deleted. Alarm name: LOG\_DEL\_FULL.

### Restore Log Files

When log files are restored (cf. Chapter 3.6, page 3-23), the log of the current day is not overwritten.

## 3.7.3 Log Viewer Window

The logs can be viewed by means of the Log Viewer application. The logged entries in the Log Viewer cannot be edited.

### Start Log Viewer

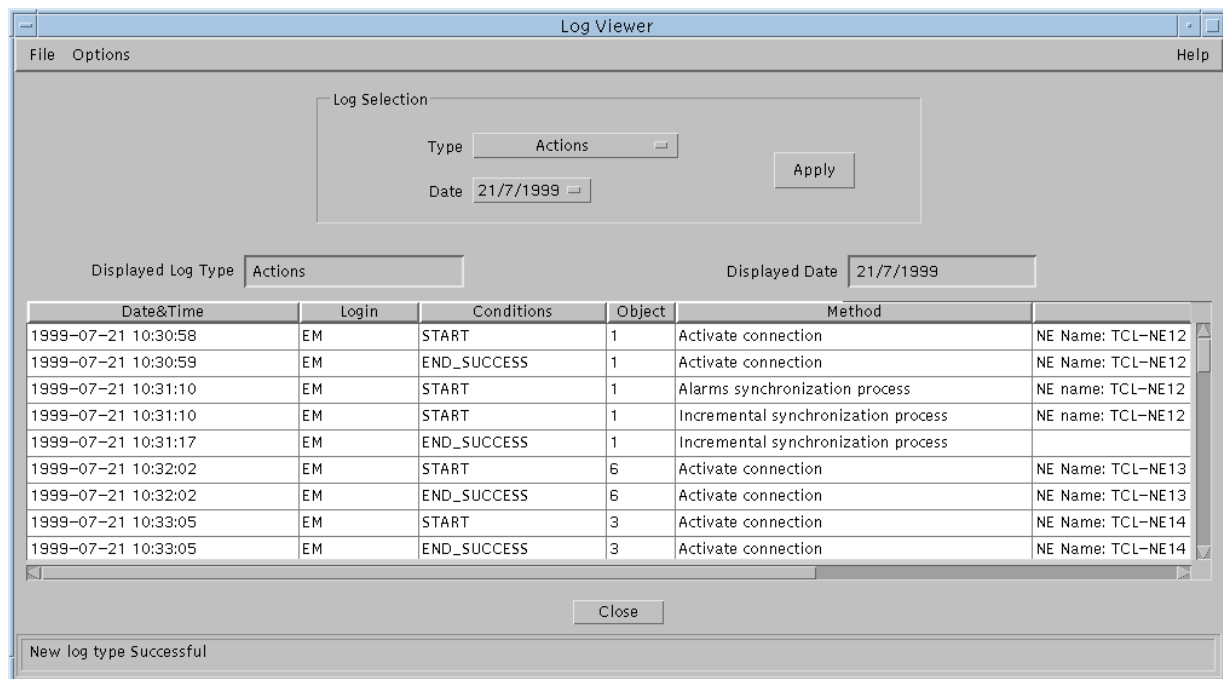
The Log Viewer is started-up by clicking on the log viewer icon in the access bar. After start-up the default log type is displayed, this value can be configured (default: "Actions").

### Access Permission

The log types which are visible to you depend on your user group. The following table shows the log types which the different user groups are allowed to see.

**Table 3-22 Visibility of a Log Type for a Certain User Group**

Log type	Visible for user group
Actions	Administrator, Maintenance
System Internal Events	Administrator, Maintenance
Autonomous Reports	Administrator, Maintenance, Monitoring



**Figure 3-12 Log Viewer**

### Meaning of Columns

The following table explains the meaning of the columns in the Log Viewer table.

**Table 3-23 Information Displayed in the Log Viewer Table**

Column	Meaning
Date&Time	Date and time when the event was registered in the log file. Format: "year-month-date hour:minute:second"
Login	The user name of the user performing an action or "EM"
Conditions	The condition of a performed action, to indicate whether it is the request or the response. (E.g. START, END_SUCCESS, END_ERROR).
Object	Unique identification of the object (NE_Id or EM) which has sent a TL1 message or has received an action.

**Table 3-23 Information Displayed in the Log Viewer Table**

Column	Meaning
Method	A string explaining the performed action.
Parameters	<ul style="list-style-type: none"> <li>■ For Actions and System Internal Events Shows all parameters involved in the action.</li> <li>■ For Autonomous Reports Shows all TL1 message parameters in the order they were received (for TL1 messages sent from NE) and all alarm fields (except Description) for platform alarms.</li> </ul>
Event Type	The event which happened in the AEM-NB.

**Log Types and Displayed Information**

Depending on the chosen log type the table in the Log Viewer displays different information (more or less columns). The following table shows which information is displayed for which log type.

**Table 3-24 Log Types**

Log Type	Contents
Actions	Date&Time, Login, Conditions, Object, Method, Parameters
System Internal Events	Date&Time, Object, Event Type, Parameters
Autonomous Report	Date&Time, Parameters, NE_Id

**Menus and Functions**

The following table provides an overview of the menus of the Log Viewer and their functions.

**Table 3-25 Menus and Functions**

Menu Item	Function
<b><i>File -&gt; New</i></b>	Start up a new Log Viewer
<b><i>File -&gt; Reload</i></b>	Update the displayed Log Viewer table with newly logged items.
<b><i>File -&gt; Print -&gt; Print Table</i></b>	Print out all logged items displayed in the table of the Log Viewer.
<b><i>File -&gt; Print -&gt; Print Window</i></b>	Print a screenshot of the whole window.
<b><i>File -&gt; Print -&gt; Preview</i></b>	Shows how it will be printed if the "Print Table" option is used. Opens directly the Print Preview window..
<b><i>File -&gt; Close</i></b>	The selected Log Viewer window is closed. Other open Log Viewer windows stay open.

Table 3-25 Menus and Functions

Menu Item	Function
<b>File -&gt; Exit</b>	Close all Log Viewer windows.
<b>Options -&gt; Default Type</b>	Set a new default type, which will be displayed, when the next Log Viewer window is opened.
<b>Help -&gt; On Window</b>	Display help for Log Viewer
<b>Help -&gt; Index</b>	Display help index.

**Actions**

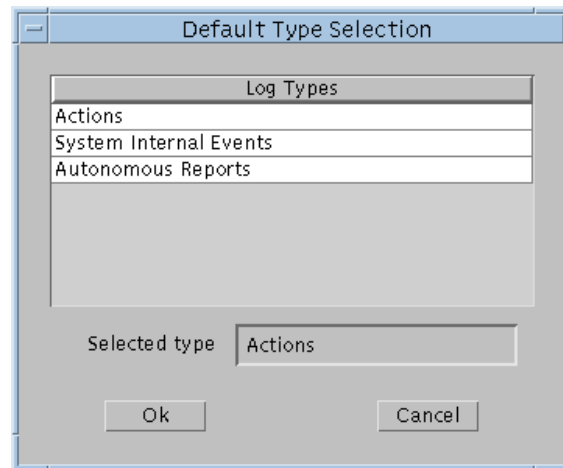
The following table lists all actions you can perform in the Log Viewer window.

Table 3-26 Actions in the Log Viewer Window

If you want to...	then...	Result
display a certain log type of a specific date	select the desired log type with the pull down control <b>Type</b> and the date of interest with the pull down control <b>Date</b> and press <b>Apply</b> .	The log of the selected type and date is displayed in the Log Viewer table.
view different log types or dates simultaneously	start another Log Viewer with <b>File -&gt; New</b> and set the desired <b>Type</b> or <b>Date</b> .	A new Log Viewer window displays the selected log type and date.
change the log type displayed at start-up	select <b>Options -&gt; Default Type</b> . In the window which opens (cf. Figure 3-13), click on the new default log type and press <b>Apply</b> or, to set no new default type, press <b>Cancel</b> .	The selected log type is displayed by default whenever a new Log Viewer window is opened.
print displayed log	select <b>File -&gt; Print -&gt; Print Table</b> or <b>File -&gt; Print -&gt; Print Window</b> .	The Log Viewer table or a screenshot of the window is printed out.
display updated log	select <b>File -&gt; Reload</b>	Newly logged entries are displayed.
sort the log	click on one of the column headers to sort the log according to the column entries alphabetically or by date and time. Click again to reverse the sort order.	The Log Viewer table is displayed sorted alphabetically or by date and time.
close one Log Viewer window	select <b>File -&gt; Close</b> or press <b>Close</b>	The selected Log Viewer window is closed.
close all Log Viewer windows	select <b>File -&gt; Exit</b>	All Log Viewer windows are closed.

**Select Default View**

The following window pops up if you have chosen to set a new default log type via **Options -> Default Type** to be displayed at every start-up of the Log Viewer. You can select a log type and press **Ok** or close the window without any actions with **Cancel**.



**Figure 3-13 Set Default Type**

## 3.8 Disaster Recovery

The AEM-NB software has built-in auto recovery features that will allow it to continue working after a problem except in the most critical situations (i.e. corrupted files, hardware failure...). In case of a disaster, the following steps should be performed by the system administrator to repair the AEM-NB and minimize the data loss.

1. Repair/replace any hardware and OS components that may be damaged. Start the system and check that the workstations and network boot properly and the users are able to log into the system.
2. Check if the AEM-NB (including all third-party software) remains installed on the machine. To list all the packages installed type:  

```
pkginfo | grep 'application Lu'
```
3. Remove all the listed packages using the **pkgrm** command (cf. Chapter 2.2.4, page 2-43).
4. Re-install the AEM-NB software. The procedure is the same as for installing the software for the first time (cf. Chapter 2.2.1, page 2-6).



### NOTE:

The packages must be re-installed in the same paths as the original installation, otherwise the data cannot be restored.

5. If any AEM-NB variable was customized, remember to reset it (the installation sets all values to default). Start the AEM-NB server and at least one client. All application windows (Users, Alarms, Configuration) should open but will show only the initial information.
6. Shut down the AEM-NB. Restore the latest backup available (cf. Chapter 3.6, page 3-23). Re-start the AEM-NB server and at least one client. Now the restored data shall be shown and the system will be back at the status prior to the latest backup.

The process between step 2 and step 6 should not take more than 4 hours. If the recovery is not successful call Lucent Technologies Technical Support.

A good backup policy is imperative in order to minimize the data loss (some examples can be found in cf. Chapter 3.6.4, page 3-28).





---

## Contents

<b>4.1</b>	<b>Introduction</b>	<a href="#"><u>4-1</u></a>
<b>4.2</b>	<b>User</b>	<a href="#"><u>4-2</u></a>
4.2.1	Create User	<a href="#"><u>4-2</u></a>
4.2.2	Modify User	<a href="#"><u>4-4</u></a>
4.2.3	Delete User	<a href="#"><u>4-6</u></a>
<b>4.3</b>	<b>Domains</b>	<a href="#"><u>4-8</u></a>
4.3.1	Create Domains	<a href="#"><u>4-8</u></a>
4.3.2	Modify Domains	<a href="#"><u>4-11</u></a>
4.3.3	Delete Domains	<a href="#"><u>4-14</u></a>
<b>4.4</b>	<b>User Groups</b>	<a href="#"><u>4-16</u></a>
4.4.1	Create User Groups	<a href="#"><u>4-16</u></a>
4.4.2	Modify User Groups	<a href="#"><u>4-21</u></a>
4.4.3	Delete User Groups	<a href="#"><u>4-26</u></a>
<b>4.5</b>	<b>Controlled Objects</b>	<a href="#"><u>4-29</u></a>
4.5.1	Modify Controlled Objects	<a href="#"><u>4-29</u></a>

---

## Contents

## 4.1 Introduction

---

This chapter describes the "User Administration and Profiling" application of the *AnyMedia*® Access System Element Manager for Narrowband Services R1.3 (AEM-NB). It allows to

- create/modify/delete users
- assign/unassign users to/from user groups
- create/modify/delete user groups
- assign/unassign user groups access to/from applications, tasks and domains
- create/modify/delete domains
- assign/unassign controlled objects to/from domains.



**NOTE:**

All actions can only be done by the AEM-NB administrator!

## 4.2 User

### 4.2.1 Create User

#### Introduction

This chapter describes the process to add a new user to the system. Before adding a new user to the system, please pay attention to the following remarks:

- The AEM-NB administrator must have a system login.
- The user must be created via OS.
- The AEM-NB administrator should know the login ID of the user to be created and the group the user shall belong to.

#### Procedure

Complete the following procedure to add a new user:

Step	Procedure
1.	Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show.



**Figure 4-1 Access Bar**

2. Select the **third** icon.  
The *User Administration* window pops up showing the *Users Table*.

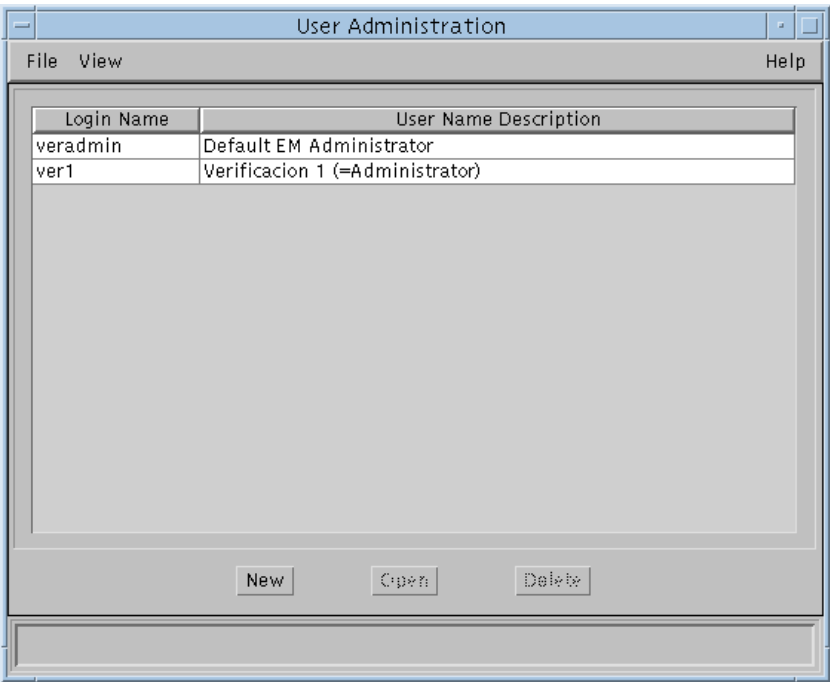


Figure 4-2 "Users Table"

- 3. Click **New**.  
The *User Profile* window pops up.

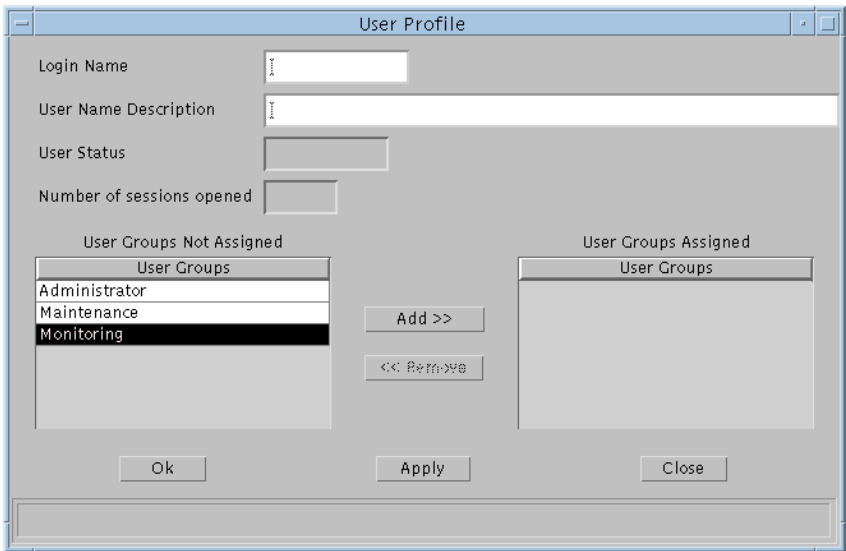


Figure 4-3 Window "User Profile"

4. Enter a new login name in the **Login Name** field (this is mandatory - 3 to 12 characters) and extra information like last name, first name, email, etc. in the **User Name Description** field (this is optional - 0 to 60 characters). Any characters are allowed.
5. Select one or more user groups the user shall belong to in the **User Groups Not Assigned** field and Click **Add**.

**NOTE:**

To create user groups see Chapter 4.4.1, page 4-16.

6. Click **OK** or **Apply** to save the settings (the system ensures that the new user does not yet exist in the system). After clicking **OK** the window will be closed.  
If you want to reject the settings, click **Close** before **OK** or **Apply**.

The other fields are described in Chapter 4.2.2, page 4-4.

## 4.2.2 Modify User

### Introduction

This chapter describes the process to modify the information or profile of a user. Before modifying the information or profile of a user, please pay attention to the following remarks:

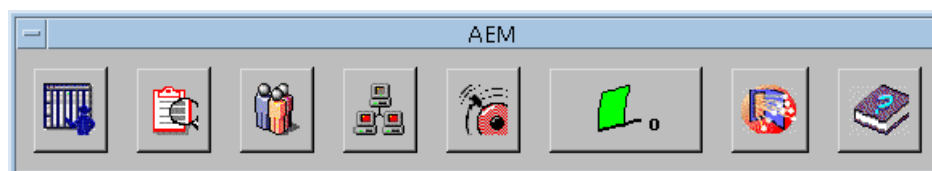
- To modify the information or profile of a user the AEM-NB administrator must have a NIS based login.
- The AEM-NB administrator is not able to change the system login information of a user, i.e. system login and password.

### Procedure

Complete the following procedure to modify the information or profile of a user:

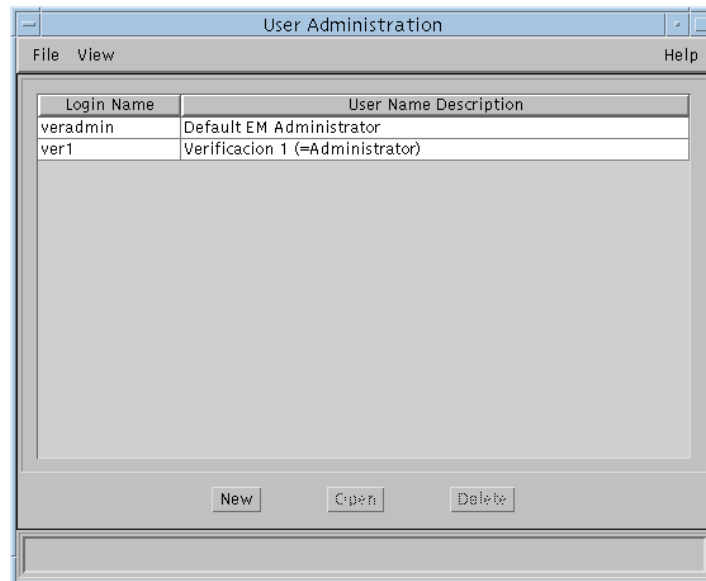
Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show. |
|----|---|



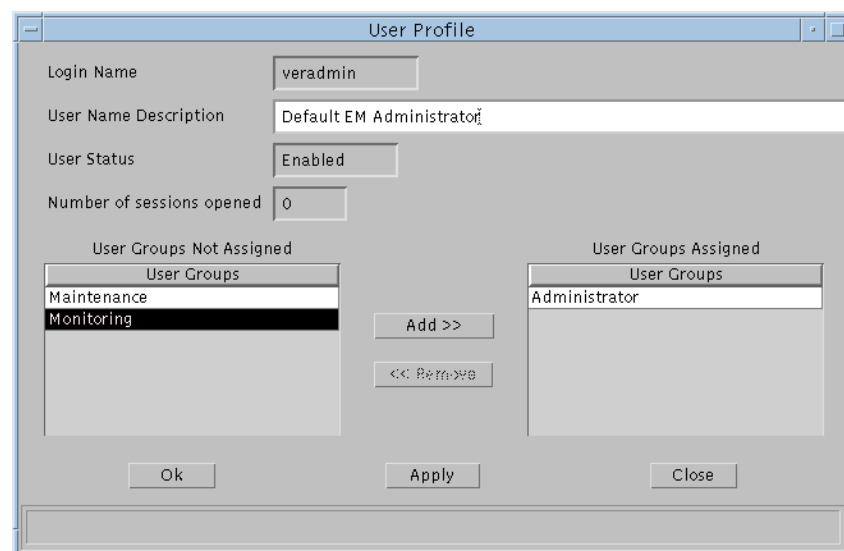
**Figure 4-4 Access Bar**

2. Select the **third** icon.  
The *User Administration* window pops up showing the *Users Table*.



**Figure 4-5** "Users Table"

3. Select one user of the **Login Name** field and click **Open**. The *User Profile* window pops up with the current information about the selected user.



**Figure 4-6** Window "User Profile"

**Change User Name Description**

To change the user name description like last name, first name, email, etc., enter the new information in the **User Name Description** field (0 to 60 characters). Any characters are allowed.

**Adding to User Groups**

To assign the selected user to further user groups, select one or more user groups in the **User Groups Not Assigned** field and click **Add**.

**NOTE:**

To create user groups see Chapter 4.4.1, page 4-16.

**Removing from User Groups**

To remove the selected user from user groups, select one or more user groups in the **User Groups Assigned** field and click **Remove**.

Click **OK** or **Apply** to save the changes. After clicking **OK** the window will be closed.

If you want to reject the changes, click **Close** before **OK** or **Apply**.

**Other Fields (read-only)**

The following fields are read-only fields to display user data:

**Login Name:**

Displays the label which identifies the user.

**User Status:**

Displays if the system login associated to this user is created (enabled) or deleted (disabled).

**Number of sessions opened:**

Displays the number of sessions opened into the AEM-NB by the user.

### 4.2.3 Delete User

---

**Introduction**

This chapter describes the process to remove a user from the AEM-NB. Before removing a user, please pay attention to the following remarks:

- To remove a user from the AEM-NB the administrator must have a system login.
- When a user is deleted, all related information and profiles are removed from the system. This does not include the system login and any other system resources such as home directories or system files which are not managed by the AEM-NB. Furthermore, the user is automatically deleted from the user groups it was included in.
- Before deleting any user assigned to the administrator user group, the AEM-NB checks that this is not the last user assigned to the administrator user group. If this is the last one assigned, the deletion is rejected.



**Procedure**

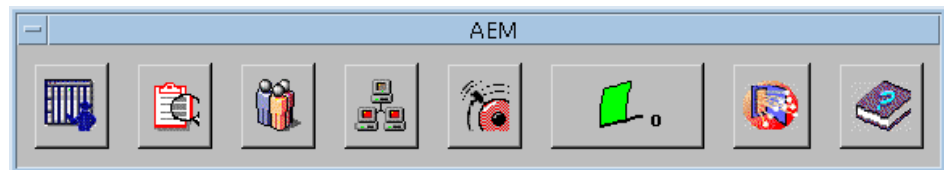
Complete the following procedure to remove a user from the AEM-NB:

---

**Step Procedure**

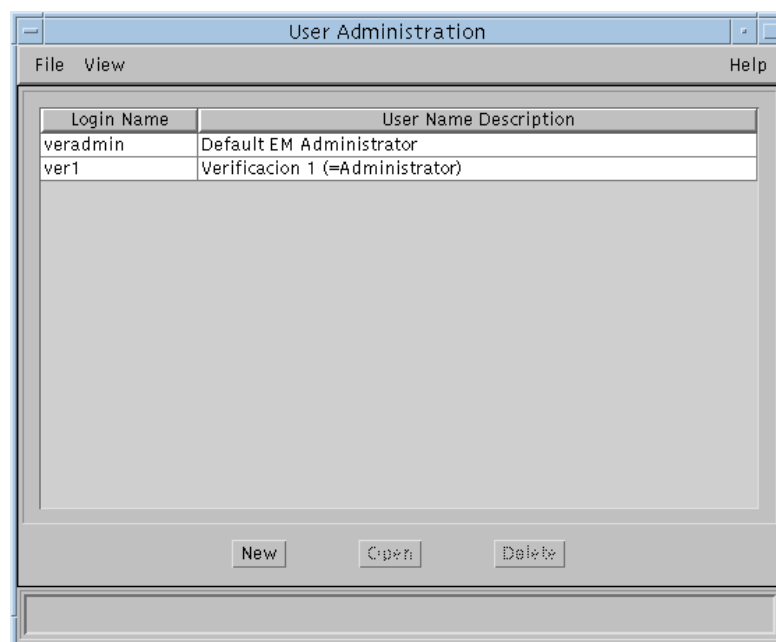
---

1. Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show.



**Figure 4-7 Access Bar**

2. Select the **third** icon.  
The *User Administration* window pops up showing the *Users Table*.



**Figure 4-8 "Users Table"**

3. Select the user which shall be deleted in the **Login Name** field and click **Delete**.
4. Confirm your selection. The window will be closed.

# 4.3 Domains

## 4.3.1 Create Domains

**Introduction** This chapter describes the process to create a new domain. Before creating a new domain, please pay attention to the following remarks:

- The AEM-NB administrator must have a system login.
- The controlled objects are defined as sets of managed NEs.
- Only "EM" and "NE" controlled object types are supported.

NOTE:  
An "EM" object is generated by default with "Type: EM" and "Value: AnyMedia" which cannot be deleted.

**Procedure** Complete the following procedure to create a new domain:

Step	Procedure
1.	Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show.



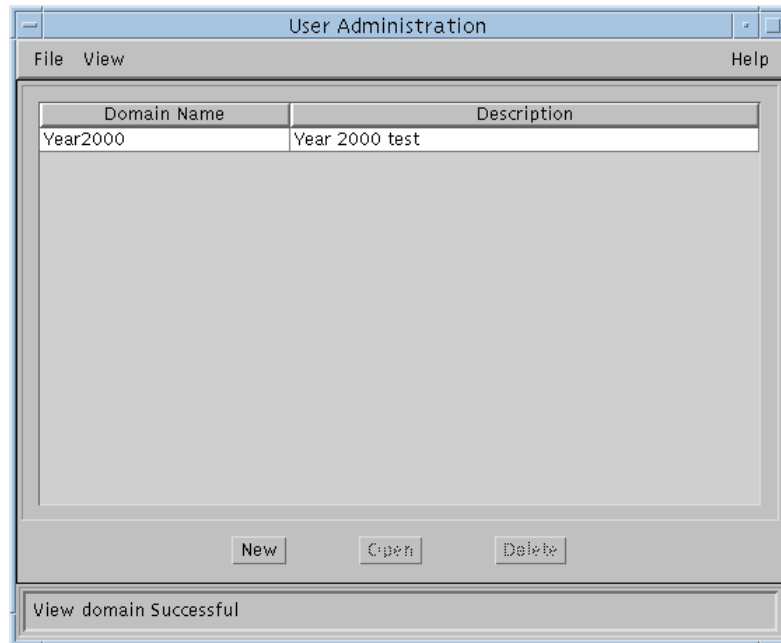
Figure 4-9 Access Bar

2. Select the **third** icon.  
The *User Administration* window pops up.



Figure 4-10 Menu Bar of Window "User Administration"

3. Select **View -> Domains**.  
The *Domains Table* appears.



**Figure 4-11 "Domains Table"**

4. Click **New**.  
The *Domain Profile* window pops up.

**Figure 4-12 Window "Domain Profile"**

5. Enter a new domain name in the **Domain Name** field (this is mandatory - 3 to 30 characters) and extra information in the **Description** field (this is optional - 0 to 60 characters). Any characters are allowed.
6. Select one or more controlled objects that shall belong to the new domain in the **Controlled Objects Not Assigned** field and click **Add**.



**NOTE:**

Each controlled object consists of two fields: *Type* and *Value*.

7. Select one or more user groups that shall have access to the new domain in the **User Groups Not Assigned** field and click **Add**.



**NOTE:**

To create user groups see Chapter 4.4.1, page 4-16.

8. Click **OK** or **Apply** to save the settings (the system ensures that the new domain does not yet exist in the system). After clicking **OK** the window will be closed.  
If you want to reject the settings, click **Close** before **OK** or **Apply**.

The other fields are described in Chapter 4.3.2, page 4-11.

## 4.3.2 Modify Domains

### Introduction

This chapter describes the process to modify the information of a domain, e.g. which devices it includes, etc. Before modifying the information of a domain, the AEM-NB administrator must have a system login.

### Procedure

Complete the following procedure to modify the information of a domain:

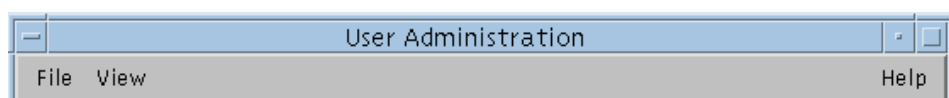
Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show. |
|----|---|



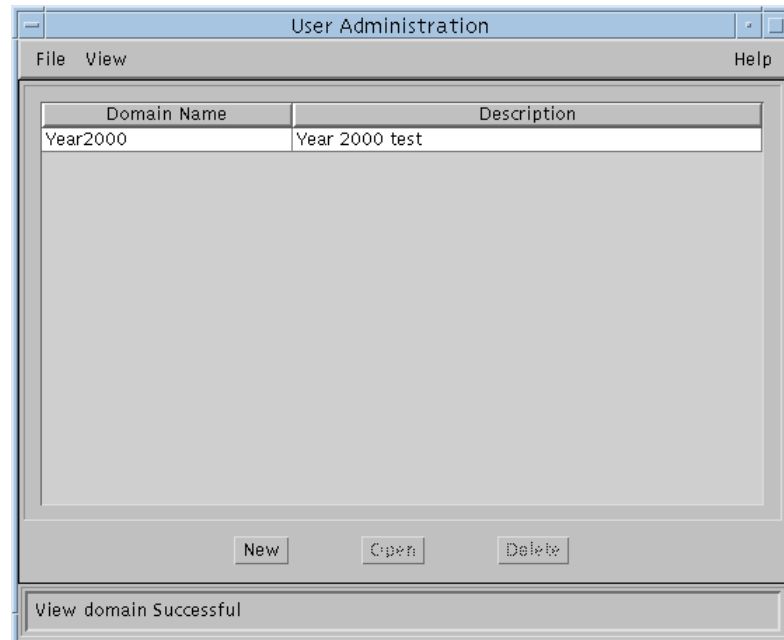
**Figure 4-13 Access Bar**

2. Select the **third** icon.  
The *User Administration* window pops up.



**Figure 4-14 Menu Bar of Window "User Administration"**

3. Select **View -> Domains**.  
The *Domains Table* appears.



**Figure 4-15** "Domains Table"

4. Select one domain in the **Domain Name** field and click **Open**. The *Domain Profile* window pops up with the current information about the selected domain.

**Figure 4-16 Window "Domain Profile"**

**Change  
Domain Name**

To change the domain name, enter the new name in the **Domain Name** field (3 to 30 characters). Any characters are allowed.

**Change Domain  
Description**

To change the domain description, enter the new information in the **Description** field (0 to 60 characters). Any characters are allowed.

**Adding  
Controlled Objects**

To assign further controlled objects to the selected domain, select one or more controlled objects in the **Controlled Objects Not Assigned** field and click **Add**.



**NOTE:**

Each controlled object consists of two fields: *Type* and *Value*.

**Removing  
Controlled Objects**

To remove assigned controlled objects from the selected domain, select one or more controlled objects in the **Controlled Objects Assigned** field and click **Remove**.

⇒ **NOTE:**  
Each controlled object consists of two fields: *Type* and *Value*.

### Adding User Groups

To give further user groups access to the selected domain, select one or more user groups in the **User Groups Not Assigned** field and click **Add**.

⇒ **NOTE:**  
To create user groups see Chapter 4.4.1, page 4-16.

### Removing User Groups

To remove assigned user groups from the selected domain, select one or more user groups in the **User Groups Assigned** field and click **Remove**.

Click **OK** or **Apply** to save the changes. After clicking **OK** the window will be closed.

If you want to reject the changes, click **Close** before **OK** or **Apply**.

## 4.3.3 Delete Domains

### Introduction

This chapter describes the process to remove a domain from the AEM-NB. Before removing a domain, please pay attention to the following remarks:

- The AEM-NB administrator must have a system login.
- Before deleting a domain, the AEM-NB ensures that there are no controlled objects assigned to this domain. If this is the case, the deletion request will be rejected.
- After a domain deletion, all related information will be removed from the AEM-NB. This does not include the devices (NEs or any other type) which are grouped in that domain or their information. Furthermore, the access permission will be automatically unassigned from the user groups that had access to this domain.

### Procedure

Complete the following procedure to remove a domain:

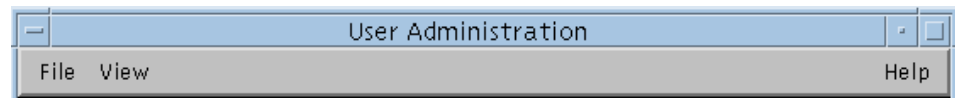
Step	Procedure
1.	Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show.



Figure 4-17 Access Bar

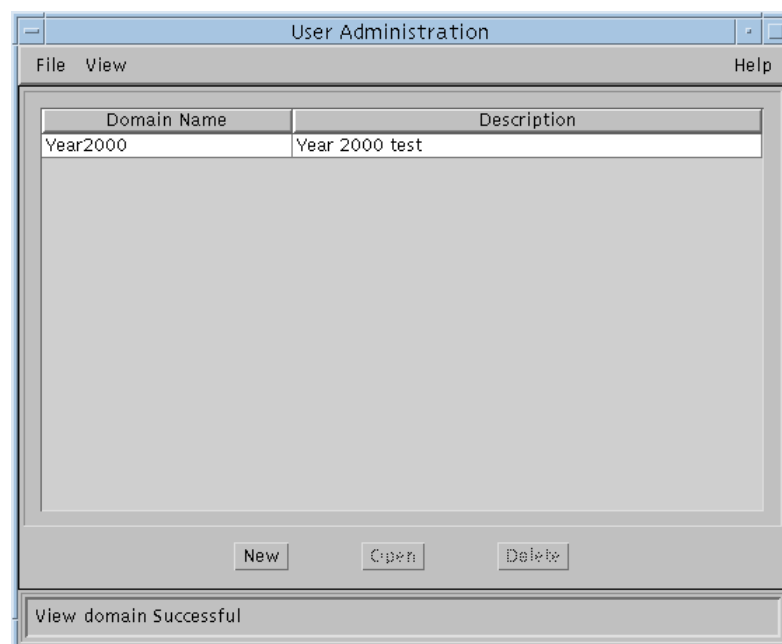


2. Select the **third** icon.  
The *User Administration* window pops up.



**Figure 4-18** Menu Bar of Window "User Administration"

3. Select **View -> Domains**.  
The *Domains Table* appears.



**Figure 4-19** "Domains Table"

4. Select the domain which shall be deleted in the **Domain Name** field and click **Delete**.
5. Confirm your selection. The window will be closed.

## 4.4 User Groups

### 4.4.1 Create User Groups

#### Introduction

This chapter describes the process to create a new user group. Before creating a new user group, please pay attention to the following remarks:

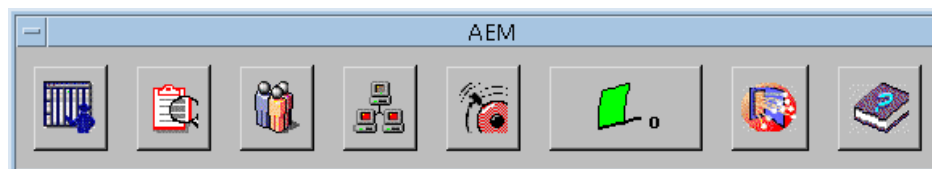
- By default the AEM-NB provides three user groups: Administrator, Maintenance and Monitoring.
- The administrator user group has access permissions to all applications and tasks.
- Before a user group can be created, modified or deleted the AEM-NB administrator must have a system login.
- Applications are divided into tasks. A user can be assigned a whole application or only a subset of its tasks.

#### Procedure

Complete the following procedure to create a new user group:

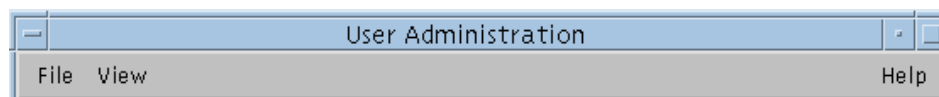
Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show. |
|----|---|



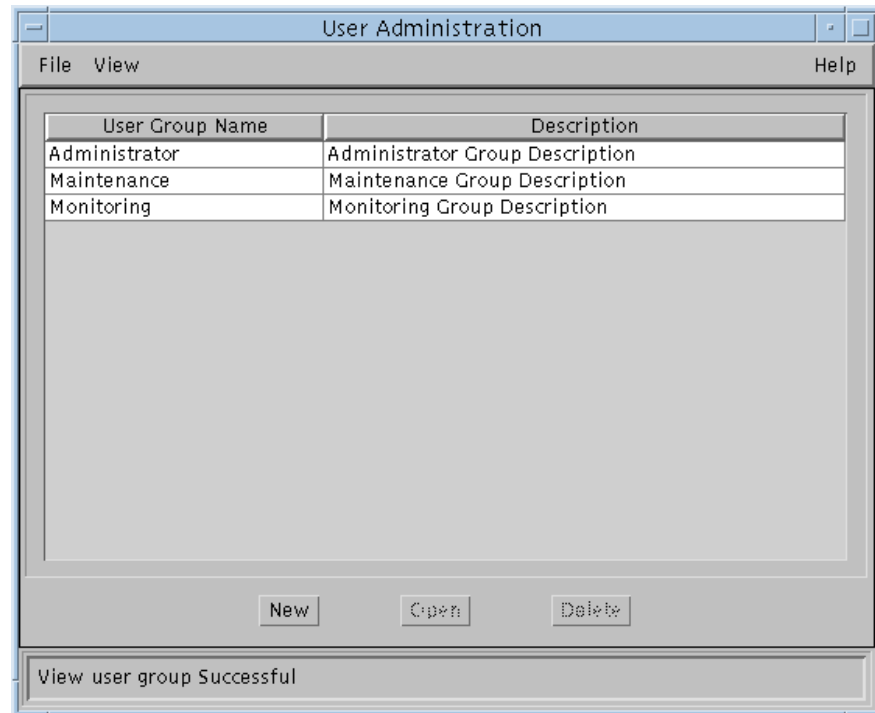
**Figure 4-20 Access Bar**

- |    |   |
|----|---|
| 2. | Select the <b>third</b> icon.<br>The <i>User Administration</i> window pops up. |
|----|---|



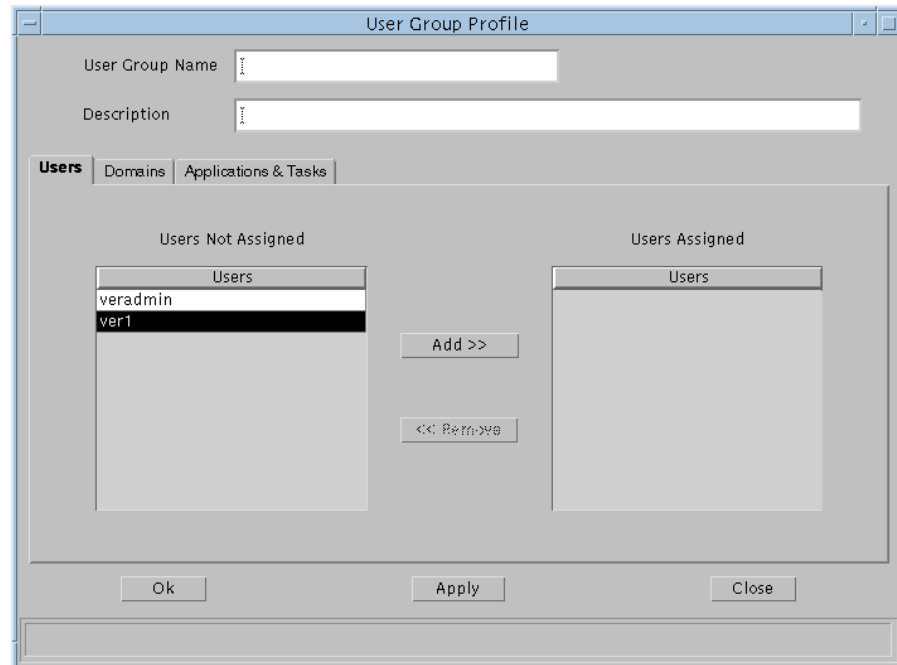
**Figure 4-21 Menu Bar of Window "User Administration"**

3. Select **View -> User Groups**.  
The *User Groups Table* appears.



**Figure 4-22** "User Groups Table"

4. Click **New**.  
The *User Group Profile* window pops up.



**Figure 4-23** Window "User Group Profile"

5. Enter a new user group name in the **User Group Name** field (this is mandatory - 3 to 30 characters) and extra information in the **Description** field (this is optional - 0 to 60 characters). Any characters are allowed.
6. Click **Users**.
7. Select one or more users that shall belong to the new user group in the **Users Not Assigned** field and click **Add**.



**NOTE:**

To create user see Chapter 4.2.1, page 4-2.

8. Click **Domains**.
9. Select one or more domains the user group shall has access to in the **Domains Not Assigned** field and click **Add**.

**NOTE:**

If access permission to a domain is granted to a user group, that permission will be automatically granted for each controlled object within that domain.

**NOTE:**

To create domains see Chapter 4.3.1, page 4-8.

For carrying out the next three steps (10, 11 and 12) please pay attention to Table 4-1. It provides an overview about the access permissions the user groups shall have.

**Table 4-1 Assignment of User Groups to Applications/Tasks**

Application	Task	User Group
System Administration	Start-up / Shutdown	Administrator
	Monitoring	Administrator
User Administration and Profiling	Access Policy Management	Administrator
	Domain Management	Administrator
Log Viewer	Actions	Administrator, Maintenance
	System Internal Events	Administrator, Maintenance
	Autonomous Report	Administrator, Maintenance, Monitoring
Alarm Viewer	Acknowledge	Administrator, Maintenance
	View <sup>a</sup>	Administrator, Maintenance, Monitoring
	Clear	Administrator, Maintenance
Configuration Manager	NE Creation	Administrator, Maintenance
	Equipment and Service Provisioning	Administrator, Maintenance
	View <sup>a</sup>	Administrator, Maintenance, Monitoring
	Test	Administrator, Maintenance, Monitoring
	Cut-through	Administrator
BroadBand EM	BroadBand EM	Administrator, Maintenance, Monitoring

- <sup>a</sup> If the VIEW task is unassigned but other tasks are still assigned, these tasks are left as assigned to this user group. But the user is not able to perform any kind of operation over these tasks until the VIEW task is assigned again.

The most of the task names are self-described, but other tasks needs a deeper description:

**Access Policy Management** provides the functionality to:

- create/modify/delete AEM-NB users
- create/modify/delete AEM-NB user groups
- create/modify/delete AEM-NB domains
- create/modify/delete assignments between AEM-NB users and AEM-NB user groups
- create/modify/delete access assignments between AEM-NB user groups and applications/tasks
- create/modify/delete access assignments between AEM-NB user groups and domains
- modify assignments between domains and controlled objects.

**Domain Management** provides the functionality to:

- modify assignments between domains and controlled objects.

**NE Creation** provides the functionality to:

- create/modify/delete controlled objects with *Type* NE.

10. Click **Applications & Tasks**.
11. Select one or more applications the user group shall has access to in the **Applications Not Assigned** field and click **Add**.  
The corresponding tasks are displayed for selection.
12. Select one or more tasks the user group shall has access to in the **Tasks Not Assigned** field and click **Add**.
13. Click **OK** or **Apply** to save the settings (the system ensures that the new user does not yet exist in the system). After clicking **OK** the window will be closed.  
If you want to reject the settings, click **Close** before **OK** or **Apply**.

The other fields are described in Chapter 4.4.2, page 4-21.

## 4.4.2 Modify User Groups

### Introduction

This chapter describes the process to modify the properties of a user group. Before modifying the properties of a user group, please pay attention to the following remarks:

- The AEM-NB administrator must have a system login.
- The administrator user group has access permissions to all applications and tasks and these access permissions cannot be modified.

### Procedure

Complete the following procedure to create a new user group:

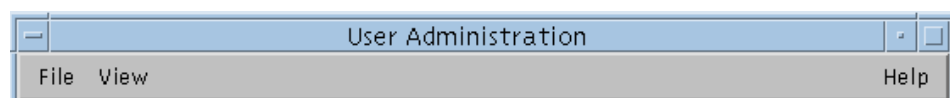
Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show. |
|----|---|



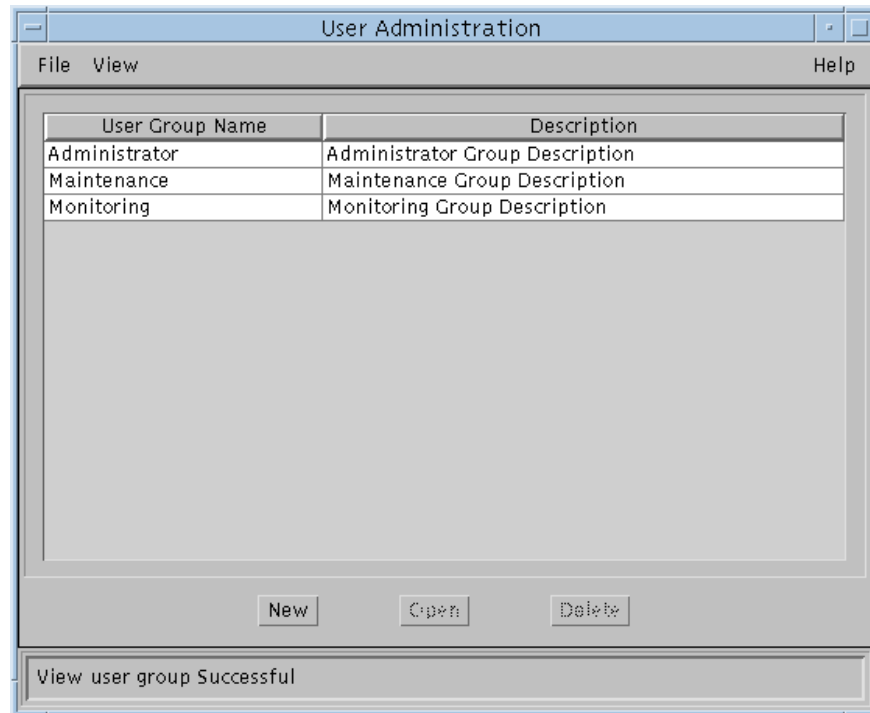
**Figure 4-24 Access Bar**

- |    |   |
|----|---|
| 2. | Select the <b>third</b> icon.<br>The <i>User Administration</i> window pops up. |
|----|---|



**Figure 4-25 Menu Bar of Window "User Administration"**

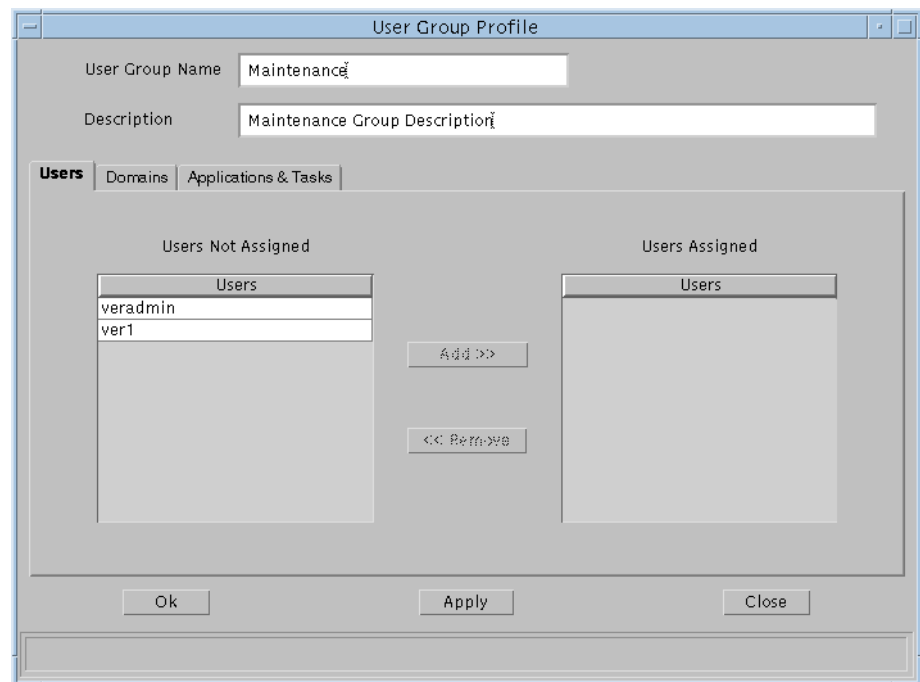
3. Select **View -> User Groups**.  
The *User Groups Table* appears.



**Figure 4-26** "User Groups Table"



4. Select one user group of the **User Group Name** field and click **Open**. The *User Group Profile* window pops up with the current information about the selected user group.



**Figure 4-27 Window "User Group Profile (Users)"**

#### **Change User Group Name**

To change the user group name, enter the new name in the **User Group Name** field (3 to 30 characters). Any characters are allowed.

#### **Change User Group Description**

To change the user group description, enter the new information in the **Description** field (0 to 60 characters). Any characters are allowed.

#### **Adding Users**

To assign further users to the selected user group, click **Users**, select one or more users in the **Users Not Assigned** field and click **Add**.



#### **NOTE:**

To a create user see Chapter 4.2.1, page 4-2.

#### **Removing Users**

To remove assigned users from the selected user group, click **Users**, select one or more users in the **Users Assigned** field and click **Remove**.



#### **NOTE:**

The last user of user group administrator is protected against deletions.

### Adding to Domains

To give the selected user group access to further domains, click **Domains**, select one or more domains in the **Domains Not Assigned** field and click **Add**.



#### NOTE:

If access permission to a domain is granted to a user group, that permission will be automatically granted for each controlled object within that domain.

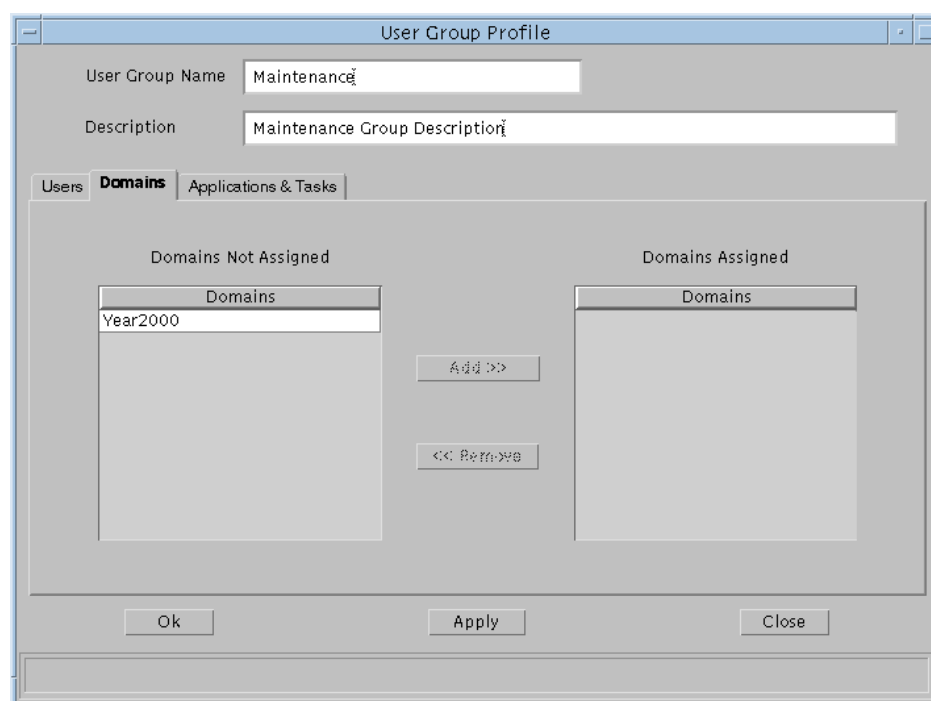


#### NOTE:

To create domains see Chapter 4.3.1, page 4-8.

### Removing from Domains

To disable the access to one or more domains, click **Domains**. The window changes its display as shown below.



**Figure 4-28 Window "User Group Profile (Domains)"**

Select one or more domains in the **Domains Assigned** field and click **Remove**.

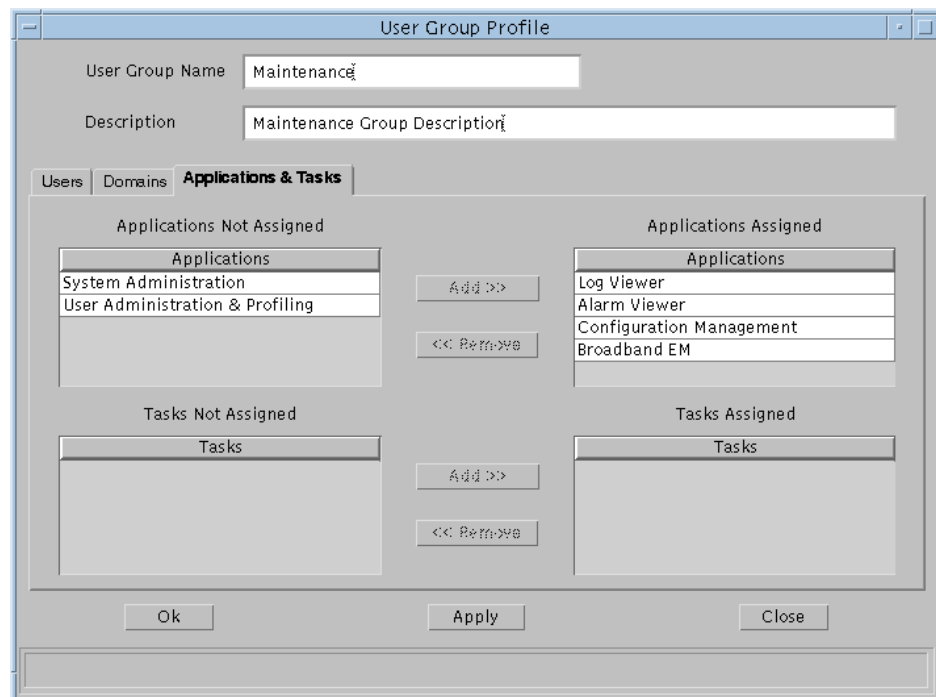


#### NOTE:

The administrator user group has access permissions to all domains and this access permissions cannot be modified.

## Adding Applications

To give the selected user group access to further applications, click **Applications & Tasks**. The window changes its display as shown below.



**Figure 4-29 Window "User Group Profile (Applications & Tasks)"**

Select one or more applications in the **Applications Not Assigned** field and click **Add**.

⇒ **NOTE:**  
For this action please pay attention to Table 4-1, page 4-19.

## Removing Applications

To disable the access to one or more applications, click **Applications & Tasks**, select one or more applications in the **Applications Assigned** field and click **Remove**. For this action please pay attention to Table 4-1, page 4-19.

⇒ **NOTE:**  
The administrator user group has access permissions to all applications and this access permissions cannot be modified.

⇒ **NOTE:**  
If the user select an application in the Applications Assigned field, all tasks that are under it will be expanded in the Tasks Assigned and Tasks Not Assigned fields.

**Adding  
Tasks**

To give the selected user group access to further tasks, select one or more tasks in the **Tasks Not Assigned** field and click **Add**.

**NOTE:**

For this action please pay attention to Table 4-1, page 4-19.

**Removing  
Tasks**

To disable the access to one or more tasks, select one or more tasks in the **Tasks Assigned** field and click **Remove**. For this action please pay attention to Table 4-1, page 4-19.

**NOTE:**

If the task "View" is removed, also the tasks "Acknowledge" and "Clear" are not possible (but not removed).

**NOTE:**

The administrator user group has access permissions to all tasks and this access permissions cannot be modified.

Click **OK** or **Apply** to save the changes. After clicking **OK** the window will be closed. If you want to reject the changes, click **Close** before **OK** or **Apply**.

### 4.4.3 Delete User Groups

**Introduction**

This chapter describes the process to remove a user group from the AEM-NB. Before removing a user group, please pay attention to the following remarks:

- The AEM-NB administrator must have a system login.
- The administrator user group is protected against deletions.
- After a user group deletion, all related information is removed from the AEM-NB. This does not include the contained users or their information, but these users will lose the ability to invoke the applications, tasks, devices and maps for which the user group had permission.

**Procedure**

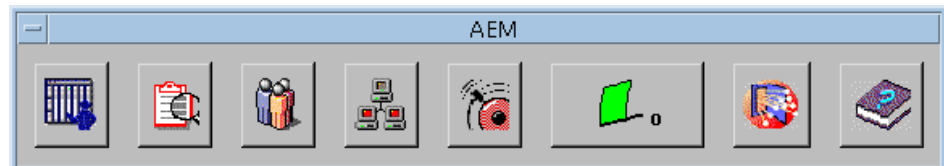
Complete the following procedure to remove a user group:

---

Step	Procedure
------	-----------

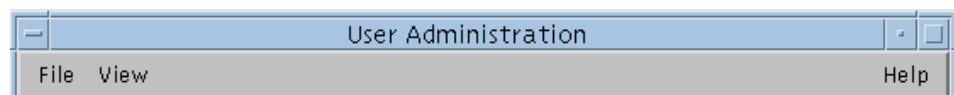
---

- |    |   |
|----|---|
| 1. | Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show. |
|----|---|
- 



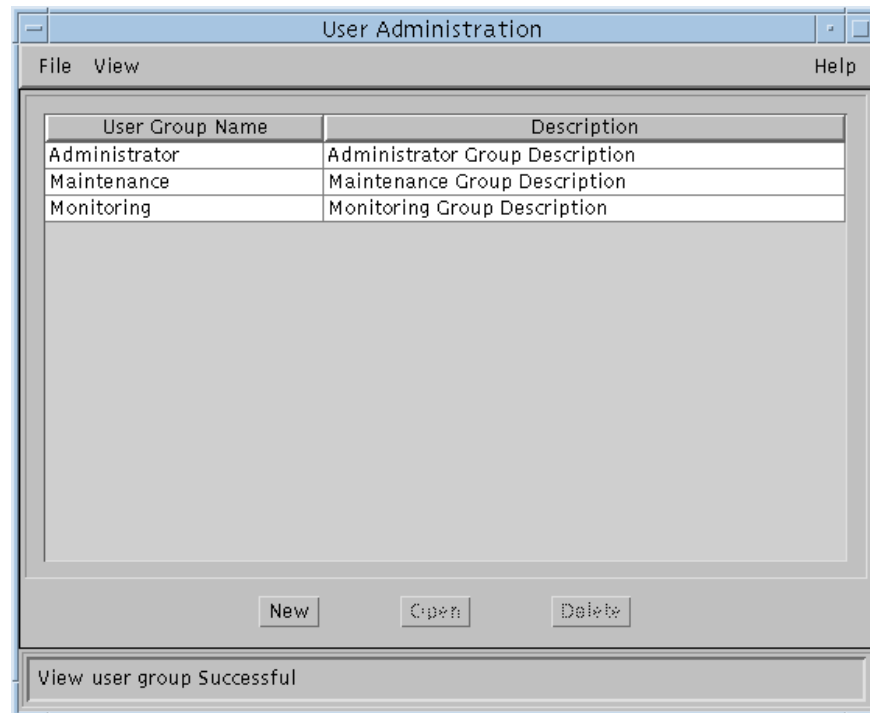
**Figure 4-30 Access Bar**

- |    |   |
|----|---|
| 2. | Select the <b>third</b> icon.<br>The <i>User Administration</i> window pops up. |
|----|---|
- 



**Figure 4-31 Menu Bar of Window "User Administration"**

- |    |   |
|----|---|
| 3. | Select <b>View -&gt; User Groups</b> .<br>The <i>User Groups Table</i> appears. |
|----|---|



**Figure 4-32 "User Groups Table"**

4. Select the user group which shall be deleted in the **User Group Name** field and click **Delete**.



**NOTE:**  
The administrator user group is protected against deletion.

5. Confirm your selection. The window will be closed.

## 4.5 Controlled Objects

### 4.5.1 Modify Controlled Objects

#### Introduction

This chapter describes the process to modify the information about existing controlled objects. The controlled object creation and deletion are not covered by this document. For NE creation and deletion refer to Chapter 5.3.1 and Chapter 5.3.8.

Before modifying the information about any controlled object the AEM-NB administrator must have a system login.

#### Procedure

Complete the following procedure to modify the information about existing controlled objects:

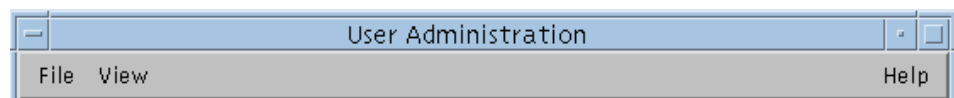
Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Login as AEM-NB administrator and start the AEM-NB access bar as described in Chapter 3.2.1. The access bar will be show. |
|----|---|



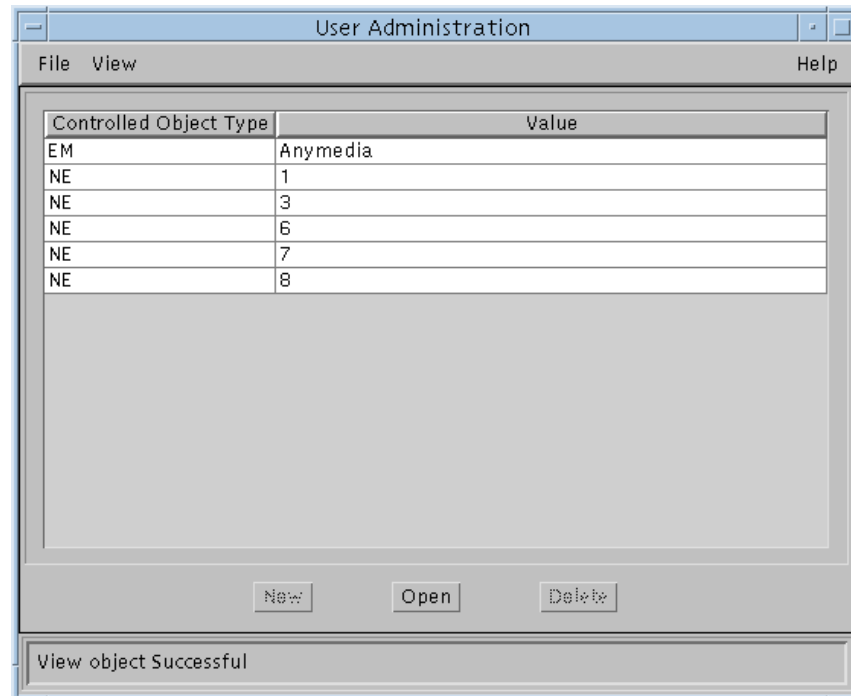
**Figure 4-33 Access Bar**

2. Select the **third** icon.  
The *User Administration* window pops up.



**Figure 4-34 Menu Bar of Window "User Administration"**

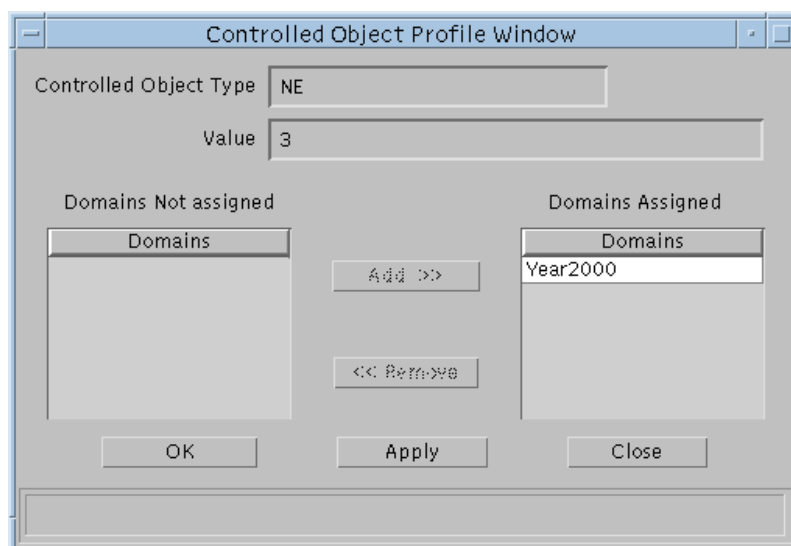
3. Select **View -> Controlled Objects**.  
The *Controlled Objects Table* appears.



**Figure 4-35** "Controlled Objects Table"



4. Select one controlled object type in the **Controlled Object Type** field and click **Open**.  
The *Controlled Object Profile* window pops up with the current information about the selected controlled object.



**Figure 4-36 Window "Controlled Object Profile"**

#### **Adding to Domains**

To assign the selected controlled object to further domains, select one or more domains in the **Domains Not Assigned** field and click **Add**.



#### **NOTE:**

To create domains see Chapter 4.3.1, page 4-8.

#### **Removing from Domains**

To remove the selected controlled object from domains, select one or more domains in the **Domains Assigned** field and click **Remove**.



#### **NOTE:**

The "EM" object generated by default is protected against deletion.

Click **OK** or **Apply** to save the changes. After clicking **OK** the window will be closed.

If you want to reject the changes, click **Close** before **OK** or **Apply**.

**Other Fields  
(read-only)**

The following fields are read-only fields to display data of the selected controlled object:

**Controlled Object Type:**

Displays the controlled object type. Possible values are *EM* and *NE*.

**Value:**

Displays the characteristics of the selected controlled object. If the controlled object is *EM* it displays "AnyMedia", if it is *NE* it displays the NE Id number.

---

## Contents

<b>5.1</b>	<b>Overview</b>	<a href="#"><u>5-1</u></a>
5.1.1	Overview of <i>AnyMedia</i> Access System R1.3	<a href="#"><u>5-1</u></a>
5.1.2	Synchronization Interfaces	<a href="#"><u>5-3</u></a>
5.1.3	OAM&P Interfaces	<a href="#"><u>5-4</u></a>
5.1.4	Alarm Interfaces	<a href="#"><u>5-4</u></a>
5.1.5	Testing Interfaces	<a href="#"><u>5-4</u></a>
5.1.6	Plug & Play Capabilities	<a href="#"><u>5-5</u></a>
5.1.6.1	NE Equipment Configuration-Related Tasks	<a href="#"><u>5-5</u></a>
<b>5.2</b>	<b>Configuration Manager Window</b>	<a href="#"><u>5-7</u></a>
5.2.1	Network Browser	<a href="#"><u>5-8</u></a>
5.2.2	Menu Bar	<a href="#"><u>5-9</u></a>
5.2.3	Status Bar	<a href="#"><u>5-11</u></a>
5.2.4	Cursor Menu	<a href="#"><u>5-12</u></a>
5.2.4.1	Structure and Cursor Menus	<a href="#"><u>5-12</u></a>
<b>5.3</b>	<b>Equipment Configuration</b>	<a href="#"><u>5-14</u></a>
5.3.1	Add a Network Element	<a href="#"><u>5-17</u></a>
5.3.2	Shelf View	<a href="#"><u>5-22</u></a>
5.3.2.1	Configuration of the Plug-ins	<a href="#"><u>5-26</u></a>
5.3.2.1.1	Configure an IO_E1	<a href="#"><u>5-26</u></a>
5.3.2.1.2	Edit E1 Feeder	<a href="#"><u>5-29</u></a>
5.3.2.1.3	Configure a COMDAC	<a href="#"><u>5-32</u></a>
5.3.2.1.4	Configure a CIU	<a href="#"><u>5-34</u></a>
5.3.2.1.5	Configure an IO_HDLC	<a href="#"><u>5-36</u></a>
5.3.2.1.6	Configure an Application Pack	<a href="#"><u>5-39</u></a>
5.3.3	Edit/View of Configuration Data	<a href="#"><u>5-45</u></a>
5.3.3.1	Network Element Synchronization	<a href="#"><u>5-45</u></a>
5.3.3.1.1	Configuration Information Synchronization	<a href="#"><u>5-45</u></a>

---

# Contents

5.3.3.1.2	Alarm Information Synchronization	<a href="#">5-46</a>
5.3.3.2	Network Element Inventory Data	<a href="#">5-49</a>
5.3.3.3	Configuration of Timing Source	<a href="#">5-52</a>
5.3.3.4	Set Date and Time	<a href="#">5-56</a>
5.3.3.5	Network Element Working Mode	<a href="#">5-57</a>
5.3.3.6	Configure Simplex COMDAC Protection Scheme	<a href="#">5-58</a>
5.3.3.7	Equipment Protection Switching	<a href="#">5-59</a>
5.3.3.7.1	COMDAC Protection Switching	<a href="#">5-60</a>
5.3.3.7.2	IO_HDLC Protection Switching	<a href="#">5-63</a>
5.3.3.8	Alarm Configuration	<a href="#">5-65</a>
5.3.4	Network Element Software Upgrade	<a href="#">5-65</a>
5.3.4.1	Network Element Software Download	<a href="#">5-65</a>
5.3.4.2	Program Copy	<a href="#">5-69</a>
5.3.5	Nonvolatile Data Storage (NVDS)	<a href="#">5-70</a>
5.3.5.1	Data Backup	<a href="#">5-71</a>
5.3.5.2	Data Restore	<a href="#">5-72</a>
5.3.6	Network Element Reset	<a href="#">5-73</a>
5.3.7	TL1 Cut-Through	<a href="#">5-74</a>
5.3.8	Delete Network Element	<a href="#">5-75</a>
<b>5.4</b>	<b>Service Provisioning</b>	<a href="#">5-77</a>
5.4.1	Create a V5 Network Interface	<a href="#">5-83</a>
5.4.1.1	Edit V5.1 Interface	<a href="#">5-87</a>
5.4.1.2	Edit V5.2 Interface	<a href="#">5-90</a>
5.4.2	Add V5 Links to V5 Interface	<a href="#">5-94</a>
5.4.2.1	Add a V5.1 Feeder	<a href="#">5-94</a>
5.4.2.2	Add a V5.2 Link	<a href="#">5-96</a>
5.4.2.3	Configure E1 Feeder List	<a href="#">5-99</a>
5.4.2.4	Configure E1 Feeder/V5 Link	<a href="#">5-101</a>
5.4.2.4.1	Create a V5 Link	<a href="#">5-101</a>
5.4.2.4.2	Edit V5 Link	<a href="#">5-104</a>
5.4.3	Add Primary V5.2 Links	<a href="#">5-109</a>
5.4.4	Add Secondary V5.2 Link	<a href="#">5-111</a>
5.4.5	Add V5 User Port	<a href="#">5-114</a>
5.4.5.1	Configure V5 PSTN User Port	<a href="#">5-118</a>
5.4.5.2	Configure V5 ISDN-BRA User Port	<a href="#">5-124</a>
5.4.5.2.1	V5 ISDN User Port Signalling Configuration	<a href="#">5-131</a>

---

## Contents

5.4.6	V5 Signalling	<a href="#">5-132</a>
5.4.6.1	Add Time Slot	<a href="#">5-136</a>
5.4.6.2	Add Communication Channel	<a href="#">5-137</a>
5.4.6.3	Edit Communication Channel	<a href="#">5-139</a>
5.4.6.4	Add Communication Path	<a href="#">5-140</a>
5.4.6.5	Cross-Connect Communication Channel with Time Slot	<a href="#">5-142</a>
5.4.6.6	Cross-Connect Communication Path with Communication Channel	<a href="#">5-144</a>
5.4.6.7	V5.2 Group 2 Protection	<a href="#">5-146</a>
5.4.6.7.1	Add V5.2 Group 2 Protection	<a href="#">5-150</a>
5.4.6.7.2	Switch V5.2 Group 2 Protection	<a href="#">5-152</a>
5.4.7	Move a V5 Interface in Service	<a href="#">5-153</a>
5.4.8	Move a V5 Link in Service	<a href="#">5-154</a>
5.4.9	Move a V5 User Port in Service	<a href="#">5-154</a>
5.4.10	Delete V5 User Port	<a href="#">5-155</a>
5.4.11	Delete V5 Link	<a href="#">5-155</a>
5.4.12	Remove Communication Channel	<a href="#">5-156</a>
5.4.13	Remove Communication Path	<a href="#">5-157</a>
5.4.14	Remove Primary Link	<a href="#">5-157</a>
5.4.15	Remove Secondary Link	<a href="#">5-158</a>
5.4.16	Remove V5 Protection Group 2	<a href="#">5-158</a>
5.4.17	Delete V5 Interface	<a href="#">5-159</a>

---

## Contents

## **5.1 Overview**

---

This chapter describes the "Configuration Manager" application of the *AnyMedia*® Access System Element Manager for Narrowband Services (AEM-NB), Release 1.3. It addresses the following topics:

- Overview of the controlled *AnyMedia* Access System.
- Explanation of menu bar and Network Browser.
- Screen navigation.
- Equipment configuration and Service provisioning.

### **5.1.1 Overview of *AnyMedia* Access System R1.3**

---

This section provides a short overview of the controlled *AnyMedia* Access System. For more information please refer to the network element documentation for R1.3.

The architecture of the *AnyMedia* AccessSystem R 1.3 is a single shelf with the following main components as shown in Figure 5-1, page 5-3:

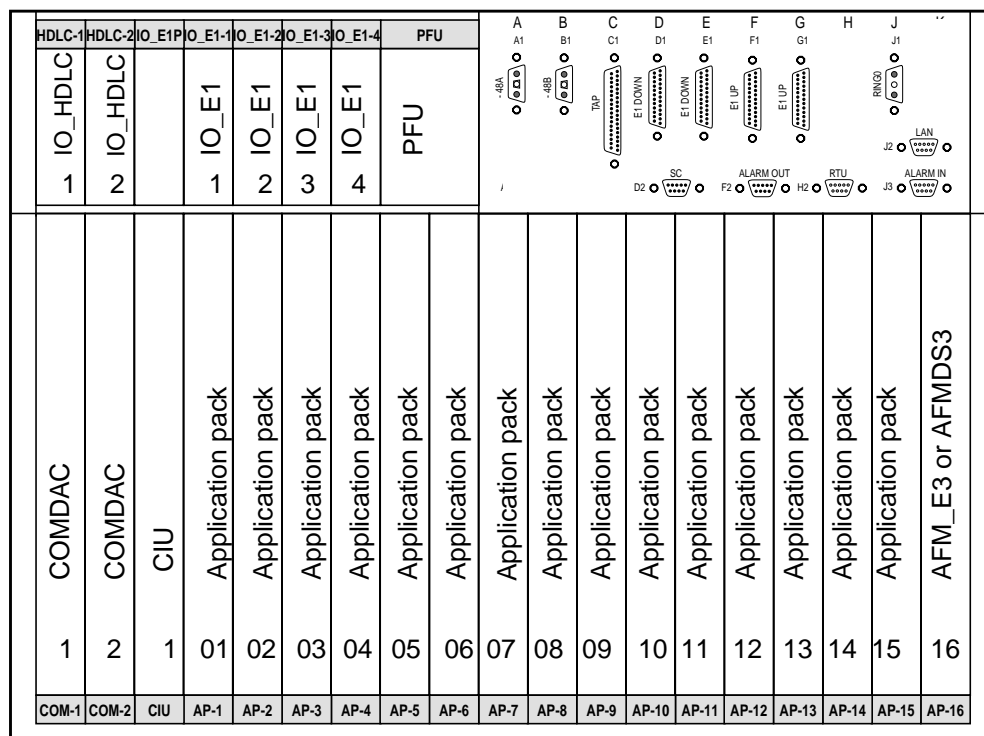
- *AnyMedia* shelf
- Power filter unit (PFU)
- Common plug-ins for narrowband services
  - Two common data and control (COMDAC)
  - One communication Interface Unit (CIU)
  - Up to four E1 interface unit (IO\_E1)
  - Two high level data link control plug-in (IO\_HDLC).

- Up to 16 application packs (AP) for narrowband services
  - LPZ100 (32 Z ports)
  - LPP100 (24 Z ports)
  - LPU112 (12 U ports).
- Test application pack 100 (TAP100)
- Plug-ins for broadband services
  - ATM Feeder Multiplexer (AFM\_E3 or AFMDS3)<sup>1</sup>
  - ADSL application pack (ADSL4 AP).
- Backplane.

1

Even when the AEM-NB directly manages only the narrowband plug-ins of the *AnyMedia* Access System, the broadband plug-ins will also be displayed to provide the required integration level between both managers.





- IO\_HDLC plug-ins for narrowband services
- IO\_E1 plug-ins for narrowband services
- COMDACs for narrowband services
- CIU for narrowband services
- AFM plug-in for broadband services (AFM\_E3 or AFMDS3)
- 15 APs may be mixed narrowband APs (POTS/ISDN) and broadband APs (ADSL4 APs)

**Figure 5-1 AnyMedia Shelf Layout (Mixed Configuration for Narrowband and Broadband Services)**

### 5.1.2 Synchronization Interfaces

For network synchronization of the narrowband part the AEM-NB recovers timing from two types of sources:

- From E1 feeders (clock derived from two of 16 E1 feeder signals)
- From an external synchronization equipment delivering a synchronization signal to the station clock interface (SCI) connected at the shelf connection panel.

Two clocks per IO\_E1 plug-in and the station clock (SC) from the SCI are connected to each COMDAC. Two of these clocks are provisioned as reference clocks.

**NOTE:**

If both reference clocks fail the system switches to free running mode.

### 5.1.3 OAM&P Interfaces

---

#### Types of OAM&P interfaces

The *AnyMedia* AccessSystem provides the following maintenance interfaces for operations, administration, maintenance, and provisioning (OAM&P):

- Craft interface terminal (CIT) port
- 10BaseT interface
- Remote operations channel (ROC).

A PC-based graphical system interface, the *AnyMedia* AccessSystem graphical system interface software for narrowband services (GSI-NB) operates over all OAM&P interfaces.

### 5.1.4 Alarm Interfaces

---

The following alarm interfaces exist for the *AnyMedia* AccessSystem:

	<ul style="list-style-type: none"> <li>■ Local alarm and status indicators</li> </ul> <p>The plug-ins have light emitting diodes (LEDs) on the faceplate to indicate status and alarm conditions. Any alarms indicated by the LEDs are reported to the GSI/EM and via the ROC if provisioned.</p>
<b>Office alarm interfaces</b>	<ul style="list-style-type: none"> <li>■ Office alarm interfaces</li> </ul> <p>Three software-controlled relays on the CIU are used as alarm outputs to indicate active alarms. The assignment to the alarm LEDs is provisionable by TL1 commands.</p>
<b>Miscellaneous alarm closure inputs</b>	<ul style="list-style-type: none"> <li>■ Miscellaneous alarm closure inputs</li> </ul> <p>The CIU supports 8 ground closure alarm inputs to indicate environmental fault conditions.</p> <p>Alarms detected at the external alarm inputs are treated in the same way as alarms detected in the AEM-NB itself. An additional LED <i>MISC</i> on the CIU faceplate indicates an active alarm input.</p>
<b>Alarm cut-off function</b>	<p>The alarm cut-off function (ACO) provides the possibility to immediately cut off the audible/visible alarms active on the alarm interface outputs. The ACO function is activated by pressing the ACO button on the CIU faceplate or with a TL1 command.</p>

### 5.1.5 Testing Interfaces

---

Two test modes can be used for testing.

- Manual testing
- Manual testing means local testing with external equipment without using the system's integrated testing capabilities.

- Interfaces for manual testing
  - Faceplate jack *DROP* on the CIU
  - Faceplate jack *CHAN/MON* on the CIU
- Integrated testing

Integrated testing means testing using only the system's integrated testing capabilities. This can be done even remotely.

  - Interfaces for integrated testing
    - TAP connector on the shelf connection panel
    - Connector on the faceplate of the test application pack (TAP100).

## 5.1.6 Plug & Play Capabilities

The plug-ins associated with the *AnyMedia* Access System have the capability to self-identify themselves with inventory data. This capability is very useful during the execution of provisioning and maintenance procedures.

For example, upon insertion of the new plug-in in the *AnyMedia* Access System shelf, the inventory data of the new plug-in, as well as its serial number, slot and plug-in entity, will be reported to the AEM-NB and/or GSI interface. The removal of any plug-in unit will be announced also.

### 5.1.6.1 NE Equipment Configuration-Related Tasks

The network element (NE) equipment configuration facilities provided by the AEM-NB cover the operations that control and provision the NE R1.3, including the following:

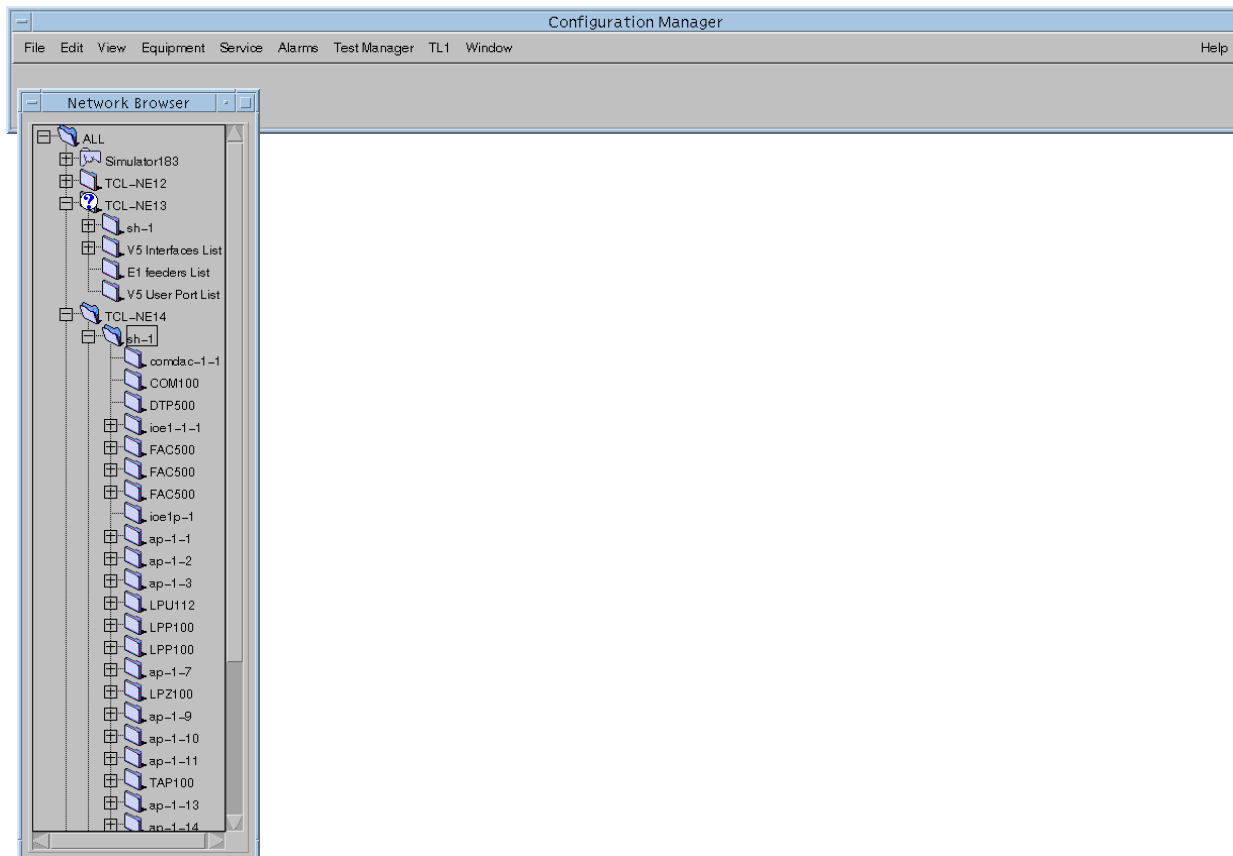
- Configuration specific equipment data, which involves tasks for:
  - NE creation & deletion
  - Plug-in management
    - COMDAC management
    - IO\_E1s management - Physical feeder management
    - IO\_HDLCs management
    - CIU management
    - AP management - Z-ports management
  - Protection management
  - Slot alarming configuration
  - Date & time management
  - NE security configuration
  - Timing synchronization provisioning.

- Maintaining a local copy of the NE inventory - which includes tasks for:
  - Initializing the local copy when an NE is add to the AEM-NB
  - Maintaining the local copy on equipment changes
  - Synchronizing the local copy with the equipment data maintained by the NE, and reporting differences.
- **Inventory Management** - system activity of collecting, updating and reporting data on *AnyMedia* Access System equipage and system status, including providing users with access to the entire equipment information, whether locally maintained or not.
- **NE Memory Administration** - this means the management of the nonvolatile data storage (NVDS) of the *AnyMedia* Access System: Backup & Restore
- **NE Software Administration** - this involves tasks to manage the nonvolatile program storage (NVPS) of the *AnyMedia* Access System: software download, copying the NVPS between controller CARS, etc.

For more information please refer to the network element documentation for R1.3.

## 5.2 Configuration Manager Window

This major application provides the user with the facilities needed to fully configure *AnyMedia* network elements (both equipment and services).



**Figure 5-2 Configuration Manager**

The initial window consists of two frames:

- At the top, a **menu bar** provides access to all possible operations on the network elements (cf. Chapter 5.2.2, page 5-9).
- On the left-hand side, the screen displays a tree-like structure (known as the **Network Browser**) with the list of NEs created and manageable by the AEM-NB (see below).

Depending on previous actions the following frames are additionally available:

- On the right-hand side, a common area is used for the display of the information requested through the menu bar, cursor menu or tool bar (if present).

- A **status bar** is incorporated at the bottom of every single screen except of Network Browser and menu bar (cf. Chapter 5.2.3, page 5-11).
- The **cursor menu** will pop up at the cursor position when the right mouse button is pressed (cf. Chapter 5.2.4, page 5-12).

### 5.2.1 Network Browser

---

The **Network Browser** displays the list of all NEs available to the user in a tree-like structure. You can select the object you want to configure, view, modify or delete. The action to be taken is selected from the menu bar or the object's pop up menu (cursor menu). By default the first time this window is opened, level two is displayed (i.e. all NEs).

By selecting an NE it is possible to gradually explode this level to display the shelf(s), slots and ports (if any), as well as network interfaces, and user ports.

#### NE Connection State

The Network Browser displays (at the NE level) an icon that identifies the connection state of each NE (not connected, not connected (trying), not connected (cancelling), connected (synchronizing) and connected).

#### Expand Display

Any level of the Network Browser (e.g NE shelf level) can be expanded into its components (e.g. cards) clicking on the "+" symbol related to the object to be expanded. Any expanded object can be collapsed clicking on the "-" symbol related to it. If the data needed to expand a level are not available (e.g. the connection state of the NE is "synchronizing") the message "data not available" will appear instead of the components. The user can collapse this message clicking on the "-" symbol of the object related to the message.



#### NOTE:

The display is not automatically refreshed. The changes are only visible after re-expand of the branch (clicking on the + sign or via menu bar View -> Expand Branch).

## 5.2.2 Menu Bar

The menu bar entries are enabled/disabled depending on the object selected in the Network Browser. The following table describes the menu bar's main entries and subsequent submenus. The right column (Available at level) identifies the Network Browser item that needs to be selected to have this menu option available to the user.

Menu entries	Available at level
<b><i>File -&gt; New -&gt; NE</i></b>	All
<b><i>View -&gt; Reload</i></b>	Window  ⇒ NOTE: This operation is not supported for the Network Browser. The menu appears only when no other Configuration Manager window is open.
<b><i>File -&gt; Open</i></b>	NE, Shelf, Slot, E1 Feeder, Drop id, V5 Interfaces List, V5 Interface id, E1 Feeder List, V5 User Port List
<b><i>File -&gt; Delete</i></b>	NE
<b><i>File -&gt; Print -&gt; Print window</i></b>	Window
<b><i>File -&gt; Print -&gt; Print table</i></b>	Window
<b><i>File -&gt; Print -&gt; Preview</i></b>	Window
<b><i>File -&gt; Exit</i></b>	Any
<b><i>Edit -&gt; Cut</i></b>	Text editing field
<b><i>Edit -&gt; Copy</i></b>	Text editing field
<b><i>Edit -&gt; Paste</i></b>	Text editing field
<b><i>Edit -&gt; Clear</i></b>	Text editing field
<b><i>View -&gt; Expand Branch (+ sign on the left)</i></b>	Any
<b><i>View -&gt; Collapse Branch (- sign on the left)</i></b>	Any
<b><i>Equipment -&gt; Provisioning -&gt; Create -&gt; NE</i></b>	All
<b><i>Equipment -&gt; Provisioning -&gt; Edit/View</i></b>	NE, Shelf, Slot, E1 Feeder
<b><i>Equipment -&gt; Provisioning -&gt; Delete</i></b>	NE

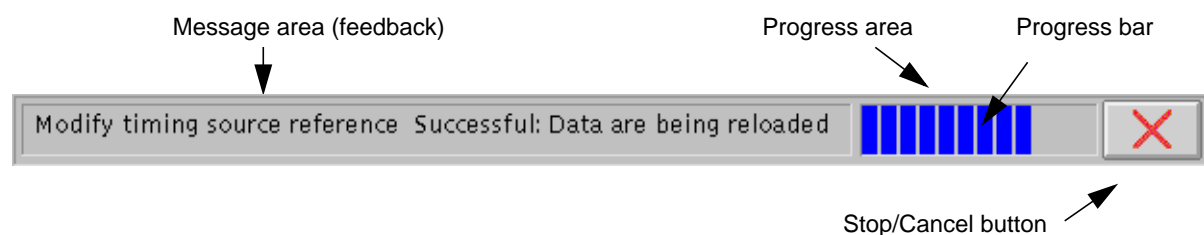
<b>Menu entries</b>	<b>Available at level</b>
<b><i>Equipment -&gt; Provisioning -&gt; Timing Source Control</i></b>	NE
<b><i>Equipment -&gt; Provisioning -&gt; Date &amp; Time</i></b>	NE
<b><i>Equipment -&gt; Provisioning -&gt; Working Mode</i></b>	NE
<b><i>Equipment -&gt; NE Inventory Data</i></b>	NE
<b><i>Equipment -&gt; EM-NE Synchronization</i></b>	NE
<b><i>Equipment -&gt; NE Reset (INIT-SYS)</i></b>	NE
<b><i>Equipment -&gt; NE SW Download</i></b>	ALL, NE (multiple selection available)
<b><i>Equipment -&gt; NE NVDS Backup</i></b>	NE
<b><i>Equipment -&gt; NE NVDS Restore</i></b>	NE
<b><i>Equipment -&gt; Shelf View</i></b>	Shelf
<b><i>Equipment -&gt; Protection</i></b>	Shelf
<b><i>Equipment -&gt; Program Copy</i></b>	Shelf
<b><i>Service -&gt; Provisioning -&gt; Create V5 Interface</i></b>	NE
<b><i>Service -&gt; Provisioning -&gt; Create V5 Link</i></b>	E1 Feeder
<b><i>Service -&gt; Provisioning -&gt; Add/Remove Link</i></b>	V5 Interface id
<b><i>Service -&gt; Provisioning -&gt; Edit/View</i></b>	V5 Interfaces List, V5 Interface id, E1 Feeder List, V5 Link (selecting E1 feeder), Drop id, V5 User Port List
<b><i>Service -&gt; V5 Interfaces List</i></b>	NE
<b><i>Service -&gt; E1 Feeder List</i></b>	NE
<b><i>Service -&gt; V5 User Ports List</i></b>	NE
<b><i>Alarms -&gt; Alarm Viewer</i></b> (cf. Chapter 6.3)	NE
<b><i>Test Manager -&gt; User Line Test</i></b> (cf. Chapter 6.4.1)	Drop id (not if the AP is a TAP)
<b><i>Test Manager -&gt; User Port Test</i></b> (cf. Chapter 6.4.2)	Drop id
<b><i>Test Manager -&gt; Standby Card Test Scheduling</i></b> (cf. Chapter 6.4.3)	Shelf
<b><i>Test Manager -&gt; TAP Test</i></b> (cf. Chapter 6.4.5)	AP (only for TAP type)
<b><i>Test Manager -&gt; CRC Test</i></b> (cf. Chapter 6.4.6)	Drop id (only for ISDN drops (LPU112))
<b><i>TL1 -&gt; Cut-through</i></b>	NE



Menu entries	Available at level
<i>Window -&gt; Show Action Bar</i>	Any
<i>Window -&gt; Cascade</i>	Any
<i>Window -&gt; Window 1</i>	Any
<i>Window -&gt; Window 2</i>	Any
<i>Help -&gt; Index</i>	Any (displays the help index for navigation through the EM help information)
<i>Help -&gt; On Window</i>	Any (case sensitive online help)

### 5.2.3 Status Bar

Feedback from the NE is displayed on screen, as is progress information related to the commands issued by the AEM-NB. This feedback is provided by the status bar incorporated at the bottom of every single screen except Network Browser and menu bar.



**Figure 5-3 Status Bar (Example)**

The status bar is composed of three sub-areas:

- **Message area:** Used to display feedback. It indicates what is being done. The last feedback message sent by the NE is displayed until a new command is sent or the window is closed.  
Example: Any time wrong data is entered in the GUI, an error message is displayed in the status bar indicating the nature of the error. By wrong data it is meant out-of-range values, inappropriate value types, etc.
- **Progress area:** Informs the user there are jobs running.
- **Stop / Cancel button:** for commands: allows cancellation of commands. Note that Cancel does not imply undo.

If you try to close the window and the last command executed has not finished yet, you will be informed (*Warning* window) that there are still jobs running:

You have running jobs. Do you want to continue?

You have to decide whether to continue or wait until the job is finished.

## 5.2.4 Cursor Menu

**Menu at the cursor position** Some objects in windows have a menu associated with them. This menu will pop up at the cursor position when the right mouse button is pressed. The cursor must not, however, be positioned on a menu bar or a window frame. The cursor menu is not available in all dialogue boxes. The functions which can be executed using this cursor menu depend on the application of the respective dialogue box.

**Select menu option** Proceed as follows to select a menu option from the cursor menu:

Step	Procedure
1.	Press and hold down the right mouse button.
2.	Drag the cursor onto the desired menu option.
Release the right mouse button to execute the menu option, or if you do not wish to execute a menu option, move the cursor away from the menu and release the right mouse button.	

### 5.2.4.1 Structure and Cursor Menus

In the following table, the last column contains the cursor menus. It also shows (*in parenthesis*) the name of the window launched if the name of the cursor menu entry and the name of the window are not the same.

Browser entries	Cursor menu entries and associated windows
<b>All</b>	Create NE ( <i>NE Information</i> ) SW Download
<b>All -&gt; NE</b>	NE Information Cut Thru ( <i>Cut Through</i> ) Delete SW Download
<b>All -&gt; NE -&gt; Shelf</b>	Shelf View Protection ( <i>Shelf Protection</i> ) Program Copy
<b>All -&gt; NE -&gt; Shelf -&gt; FAC500 <sup>a</sup></b>	Edit ( <i>IO_E1</i> )
<b>All -&gt; NE -&gt; Shelf -&gt; FAC500-&gt; E1 Feeder</b>	Edit ( <i>E1 Feeder/V5 Link</i> ) Create V5 Link ( <i>E1 Feeder/V5 Link</i> ) - only if the E1 Feeder is free

<b>Browser entries</b>	<b>Cursor menu entries and associated windows</b>
<i>All -&gt; NE -&gt; Shelf -&gt; IDC500<sup>b</sup></i>	Edit ( <i>IO_HDLC</i> )
<i>All -&gt; NE -&gt; Shelf -&gt; COM500<sup>a</sup></i>	Edit ( <i>COMDAC</i> )
<i>All -&gt; NE -&gt; Shelf -&gt; DTP500<sup>a</sup></i>	Edit ( <i>CIU</i> )
<i>All -&gt; NE -&gt; Shelf -&gt; LPZ100B (LPP100B, LPU112, TAP100, slot id)<sup>b</sup></i>	Edit ( <i>AP</i> ) TAP Test (only if selected object is TAP card)
<i>All -&gt; NE -&gt; Shelf -&gt; LPZ100B (LPP100B, LPU112, TAP100) -&gt; Drop id</i>	Edit ( <i>V5 PSTN/ISDN User Port</i> ) User Port Test Line Test (except for TAP100 ports) CRC Test (for ISDN drops from LPU112) Loopback (for ISDN drops from LPU112)
<i>All -&gt; NE -&gt; V5 Interfaces List</i>	Create V5 ( <i>V5 Interface Create</i> ) Edit ( <i>V5 Interfaces List</i> )
<i>All -&gt; NE -&gt; V5 Interfaces List -&gt; V5 Interface id</i>	Edit ( <i>V5.1/V5.2 Interface</i> ) Add/Remove Links ( <i>V5.1 Set Feeder</i> ), ( <i>V5.2 Add/Remove Links</i> )
<i>All -&gt; NE -&gt; E1 Feeder List</i>	Edit ( <i>E1 Feeder List</i> )
<i>All -&gt; NE -&gt; V5 User Port List</i>	Edit ( <i>V5 User Port List</i> )

a If there is no card inserted the slot id will be displayed instead of the apparatus code.

b If the slot has not been provisioned the slot id will be displayed instead of the apparatus code.

## 5.3 Equipment Configuration

### Overview

Configuration of specific equipment data is the process of preparing the AEM-NB for control of the *AnyMedia* Access System by configuring and setting any required option.

Prior to network interface configuration and service configuration, the AEM-NB must know some data of the equipment; this is done during the NE creation process, which is usually followed by plug-in configuration.

Then, during NE management, some other tasks regarding equipment configuration can be performed by the AEM-NB, e.g. Date & Time Management, Timing Synchronization Management, Protection Management, etc.

Finally, if the NE is not managed by the AEM-NB any longer, it shall be deleted from the AEM-NB database.

Even when autonomous notifications are provided when changes occur to the NE inventory database as a result of changes in the physical inventory, i.e. an AP is plugged in or removed, the *AnyMedia* Access System R1.3 uses a provisioning model to provide service, which means that the circuit must be prepared to provide service by defining its function and setting any required options.

For example, for creation of a POTS or ALL service for a subscriber line at first a POTS AP has to be provisioned. For Integrated Service Digital Network (ISDN) services an IO\_HDLC plug-in has to be provisioned.

AP provisioning will be performed to establish a desired POTS plug-in type in a desired slot xx (e.g. enter-ap <lpz100>). Even when to be fully functional an AP must be, not only inserted but also provisioned, and the provisioned card type must fit the actual type of the inserted plug-in, this process does not require any predefined order, that is, a card can be provisioned and configured by the AEM-NB even when the slot is still empty.

The description of equipment configuration is divided in three main sections:

- Add NE (cf. Chapter 5.3.1, page 5-17)
- Edit/view configuration data (cf. Chapter 5.3.3, page 5-45)
- Delete NE (cf. Chapter 5.3.8, page 5-75).

### Screen Navigation

Figure 5-3 shows an overview of the screen navigation for equipment configuration. In this figure is assumed that the NE is already connected (cf. Chapter 5.3.1, page 5-17).

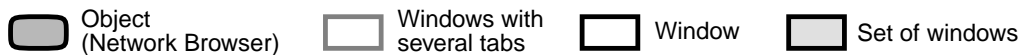
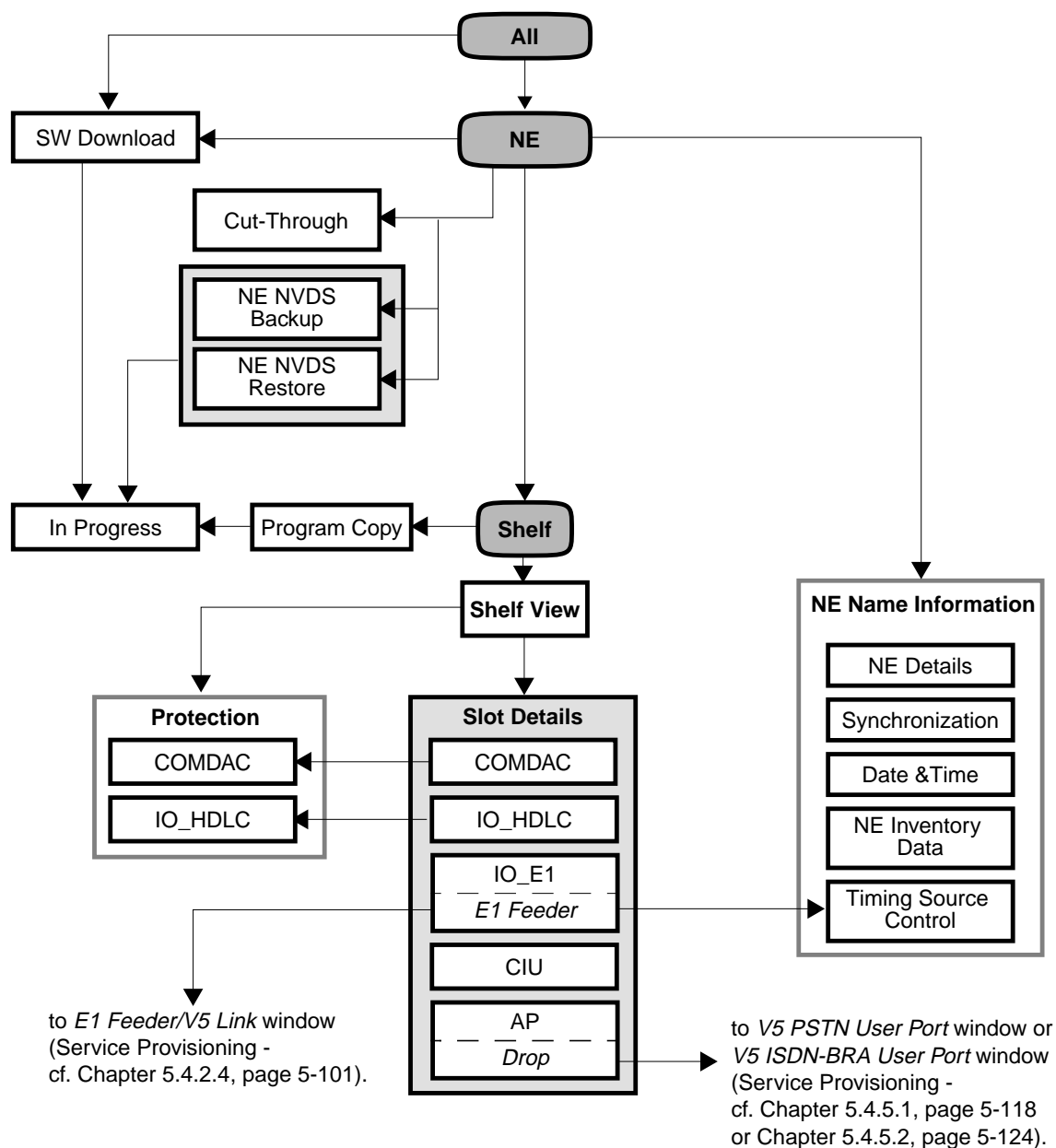
The boxes with a gray background show the Network Browser selection the other boxes show the possible menus that can be reached by using the menu bar or the cursor menu.

The arrows represent the order in which the windows can be opened.

**Examples**

To open the *COMDAC Shelf Protection* window proceed as follows:

- Select ***ALL -> NE -> Shelf*** via the Network Browser and select ***Equipment -> Protection*** via the menu bar or
- Select ***ALL -> NE -> Shelf*** via the Network Browser and select ***Protection*** via the cursor menu.



**Figure 5-3 Screen Navigation for Equipment Configuration**

### 5.3.1 Add a Network Element

---

The following steps are necessary to add an NE:

- Create NE
- Assign Domain
- Connect NE.

#### Assumptions

To add an NE the following assumptions must be fulfilled:

- The PC-based GSI is used to set the NE in a state where NVDS (Non-Volatile Data Storage) is populated with the minimum values (i.e. target id, IP-address, user id).
- All those parameters are assumed to be known by the user.
- The DCN (Data Communication Network) link with the NEs is available (cf. Appendix).
- Domains are already created (cf. Chapter 4.3.1, page 4-8).



#### NOTE:

The windows shown in this chapter are merely meant as an example. The contents (text) within a window, as well as the window itself, may slightly differ from the window as shown on your system.

**Add NE Procedure**

Complete the following procedure to add an NE.

---

Step	Procedure
------	-----------

---

1. Select **ALL** in the Network Browser and **Create NE** via the cursor menu or select **File -> New -> NE** or **Equipment -> Provisioning -> Create -> NE** via the menu bar.  
The *NE Name Information* window pops up:

The screenshot shows a window titled "New NE" with a tabbed interface. The "NE Details" tab is selected. It contains four main sections: "NE Data" with input fields for "NE Name" and "NE id" and an "Apply" button; "Communication Info" with input fields for "IP Address" and "TID" and an "Apply" button; "Authentication" with input fields for "Login" and "Password" and an "Apply" button; and "Connection" with a "Connection State" field displaying "Not Connected" and a "Connect" button. A "Close" button is located at the bottom center, and a red "X" icon is in the bottom right corner.

**Figure 5-4 "NE Name Information" Window**

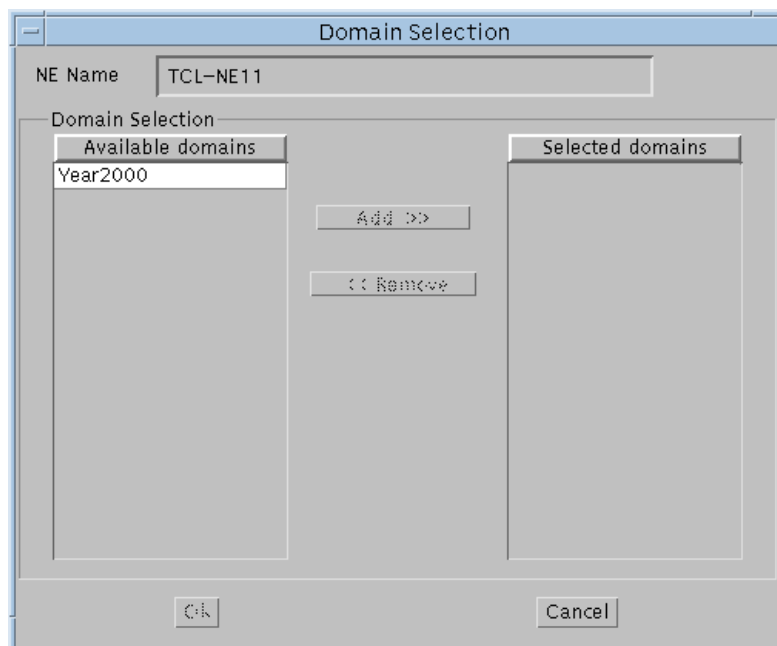
While creating a new NE the tab **NE Details** is active by default.

2. Enter an appropriate **NE name** in the corresponding field. All characters are allowed, the maximum length is 30 characters. (At this stage the fields **Communications Info**, **Authentication** and **Connection** are not available.)

The field **NE id** shows a unique identifier used internally used by the AEM-NB.

3. Press **Apply** to confirm. The *Domain Selection* window pops up.





**Figure 5-5 "Domain Selection" Window**

### Assign Domain

At creation time, the NE must be included in one or several domains (for domain creation see chapter 4). The *Domain Section* window consists of two lists: **Available Domains** and **Selected Domains**. This window provides the user with the facilities needed to select the domains from which the NE will be accessible.

4. Use the **Add >>** button to move the selected NE from the **Available Domains** list box to the **Selected Domains** one. Use **<< Remove** to remove domains from the **Selected Domains** list.  
(The **Add >>** button and the **<< Remove** button are available only after having selected a domain name from the corresponding list.)
5. Press **OK** to confirm.  
In the *NE Name Information* window the fields **Communications Info**, **Authentication** and **Connection** are displayed now. The **Connection State** is set to **Not Connected** (see step 7).



#### NOTE:

If you decide to close this window (via **Cancel** or window controls), a *Warning* window pops up informing you of the possible rejection of the NE creation:

**At least 1 domain must be selected. Otherwise the NE creation operation will be rejected. Do you want to go back to Domain Selection?**

If you select **No**, the creation of the NE is rejected. Otherwise, the *Domain Selection* window is activated. The window remains on the screen until you make a decision.

## Connect NE



### NOTE:

To establish the connection to the created NE first you have to enter the appropriate data in the fields **Communications Info** and **Authentication** in the *NE Name Information* window. After that it is possible to establish the connection by pressing **Connect**. Depending on the **Connection State** this Label button provides different functions: **Connect**, **Disconnect**, **Cancel**

6. Enter the **IP Address** and **TID** (Target ID, the name of the NE to which the connection is addressed) of the new NE in the field **Communications Info**. IP Address format: xxx.xxx.xxx.xxx; where x is a numeric [0, 9]; the TID has a range from 1 to 20 characters.



### NOTE:

Once the connection is established, these fields can not be edited unless the connection is broken.

7. Press **Apply** to confirm.
8. Enter the **Login** and **Password** in the **Authentication** pane.



### NOTE:

Once the connection is established, these fields can not be edited unless the connection is broken.

9. Press **Apply** to confirm.



### NOTE:

Now the connection can be established. The Label button in the field **Connection** displays **Connect**.

10. Press **Connect** to establish the connection.  
If all entries were correct the connection will be established and the new NE can be displayed on the Network Browser.  
Wrong entries (incorrect login or password) will result in an error message.



### NOTE:

The field **Connection State** reflects the current connection state with the NE (Not Connected, Not Connected (Trying), Connected (Synchronizing) and Connected).

The label button on the right hand side can be used to change the connection state (**Connect**, if the connection state is Not Connected; **Disconnect**,

if the connection state is Connected or Connected (Synchronizing); **Cancel**, if the connection state is Not Connected (Trying).

Edit and provisioning actions are only possible once the connection is established. Only in this case can the NE be displayed on the Network Browser.

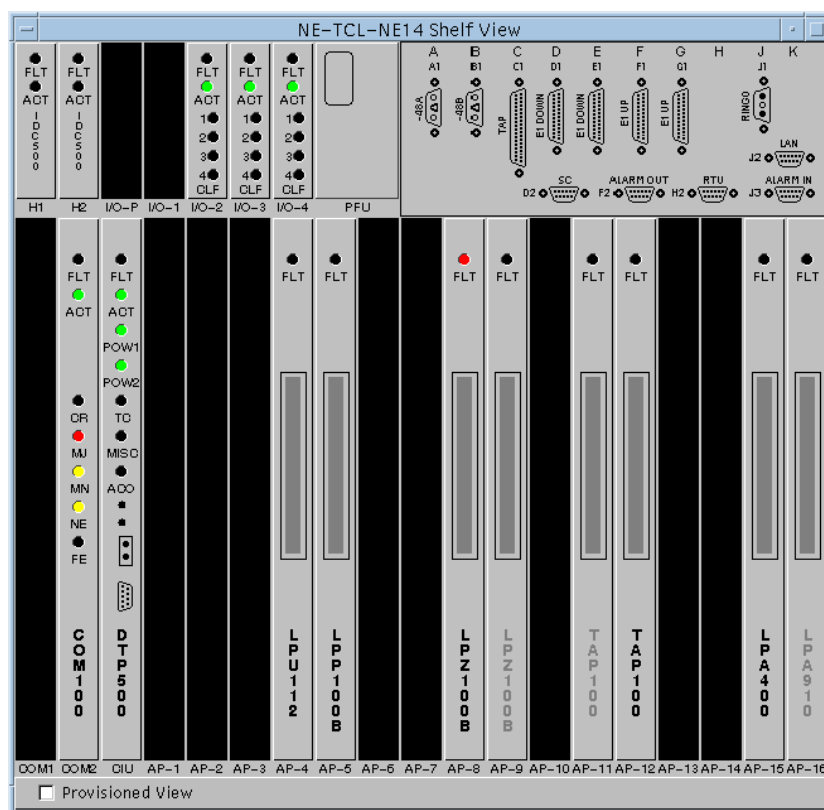
Adding an NE is normally followed by setting timing source (cf. Chapter 5.3.3.3, page 5-52) and configuring simplex COMDAC protection (cf. Chapter 5.3.3.6, page 5-58).

### 5.3.2 Shelf View

The purpose of this tab of the *NE Name Information* window is to provide a simple graphical representation of the NE shelf.

Complete the following procedure to display the shelf view:

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; Shelf</b> in the Network Browser and <b>Shelf View</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Shelf View</b> via the menu bar. The <i>Shelf View</i> window pops up.



**Figure 5-6** "Shelf View" Window

This window provides general inventory information as well as provisioning and alarm information (through the LEDs). Each slot will show either the apparatus code of the inserted card (default view) or the apparatus code provisioned in that slot (provisioned view) or no apparatus code otherwise. If the slot is empty, no card will be shown, otherwise, the slot will display the faceplate of the inserted card with its LEDs (if applicable).

Single clicking on any slot will launch the card-specific window even when the card is not inserted.:

	Apparatus Code	Card Type
Plug_ins	COM500	COMDAC, cf. Chapter 5.3.2.1.3, page 5-32
	DTP500	CIU, cf. Chapter 5.3.2.1.4, page 5-34
	IDC500	IO_HDLC, cf. Chapter 5.3.2.1.5, page 5-36
	FAC500	IO_E1, cf. Chapter 5.3.2.1.1, page 5-26
Applications packs	LPZ100B	ZAP 100 S2, cf. Chapter 5.3.2.1.6, page 5-39
	LPP100B	PPM_12/16, cf. Chapter 5.3.2.1.6, page 5-39
	LPU112	ISDN12_U, cf. Chapter 5.3.2.1.6, page 5-39
	TAP100	TAP, cf. Chapter 5.3.2.1.6, page 5-39
Broadband applica- tions	LPA900	AFM_DS3
	LPA910	AFM_E3
	LPA400	ADSL4.

The *Shelf View* window displays different colors for different types of LEDs. The following table describes the colors that are used for each LED type inside every card type. The table describes the colors used when the LED is ON or blinking. If the LED is OFF, the color black is used.

Plug-in	LED	Color	Meanings
IO_E1	FLT	red	<ul style="list-style-type: none"> <li>■ Lit during plug-in failure.</li> <li>■ Flashes when the plug-in executes off-line self-test.</li> </ul>
	ACT	green	Lit when the plug-in is service-active.
	CLF1	yellow	Lit when a fault or facility alarm occurs on the in service received E1 port 1.
	CLF2	yellow	Lit when a fault or facility alarm occurs on the in service received E1 port 2.
	CLF3	yellow	Lit when a fault or facility alarm occurs on the in service received E1 port 3.
	CLF4	yellow	Lit when a fault or facility alarm occurs on the in service received E1 port 4.

Plug-in	LED	Color	Meanings
COMDAC	FLT	red	<ul style="list-style-type: none"> <li>■ Lit when a fault is detected on the plug-in.</li> <li>■ Flashes during software download and turnup.</li> </ul>
	ACT	green	Indicates that this COMDAC is active.
	CR	red	Lit when the highest severity alarm is critical.
	MJ	red	Lit when the highest severity alarm is major.
	MN	yellow	Lit when the highest severity alarm is minor.
	NE	yellow	Lit when the source of the fault or abnormal condition is near end.
	FE	yellow	Lit when the source of the fault or abnormal condition is far end.
CIU	FLT	red	Lit when a fault is detected on the plug-in.
	ACT	green	Lit when a test is in progress. Plug-in id in operation.
	POW1	green	Lit when -48V. Power supply A is in operation.
	POW2	green	Lit when -48V. Power supply B is in operation.
	TC	green	Lit when test is in progress (TAP100 connected).
	MISC	yellow	Lit when one of the eight miscellaneous alarm inputs is active.
	ACO	green	Alarm Cut-off reminder
Application Packs	FLT	red	<ul style="list-style-type: none"> <li>■ Lit when a fault is detected on the AP</li> <li>■ Flashes when the AP executes off-line shelf-tests.</li> </ul>
IO_HDLC	FLT	red	<ul style="list-style-type: none"> <li>■ Lit when a fault is detected on the plug-in</li> <li>■ Flashes when the plug-in executes off-line shelf-test.</li> </ul>
	ACT	green	Lit when the plug-in is service-active.

See Chapter 6.2, page 6-1 for more details about alarm handling.

For cards which need to be provisioned (APs and IO\_HDLCs) it is necessary to represent the slot state since the provisioned data may be different to the inserted card. There are two possible views of this window:

- Inserted view (apparatus codes of inserted cards are shown)
- Provisioned view (apparatus code of the provisioned cards is shown).

The user can switch between the two views via a check box located in the toolbar of this window.

The following table describes the representation of the different slot states:

Slot State	Description and Representation	Inserted View		Provisioned View	
		Plug-in	Label	Plug-in	Label
provisioned, inserted and match	The type of the provisioned card is the same as the type of the inserted card.	grey	black	grey	black
provisioned, inserted and mismatch	The type of the provisioned card is different from the type of the inserted card.	grey	dark grey	gray	dark grey
provisioned and not inserted	The operator has provisioned this slot associating it to a type of card but no card is inserted in the slot.	black	-	black	white
not provisioned and inserted	No card type is pre-provisioned in the slot but a card is inserted.	grey	dark grey	gray	-
not provisioned and not inserted	No card type is provisioned and no card is inserted in the slot.	black	-	black	-

⇒ **NOTE:**  
"Plug-in" refers to the slot faceplate, "Label" refers to the apparatus code.

⇒ **NOTE:**  
The NE does not send the "match" indication for a provisioned broadband AP. The shelf view therefore indicates "provisioned, inserted and mismatch" until a re-sync is done.

### 5.3.2.1 Configuration of the Plug-ins

#### 5.3.2.1.1 Configure an IO\_E1

The IO\_E1 plug-in provides four physical E1 interfaces to accommodate telephony via standard V5 network interfaces.

#### Procedure

Complete the following procedure to view/edit the IO\_E1 data:

Step	Procedure
------	-----------

- |    |  |
|----|--|
| 1. | <p>Select <b>All -&gt; NE -&gt; Shelf -&gt; FAC500</b> in the Network Browser and <b>Edit</b> via the cursor menu</p> <p>or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> via the menu bar</p> <p>or single click on the plug-in <b>IO_E1</b> in <b>Shelf View</b> window.</p> <p>The <b>IO_E1</b> window pops up:</p> |
|----|--|

IO-E1

NE Name: TCL-NE14

Slot: ioe1-1-3

Inventory Information

Card Type: IOE1      Serial Number: 99OC02100154

Apparatus Code: FAC500      ICC: 1-2

CLEI:      ECI:

E1 Information

Feeder	V5 Interface Id	V5 Link id
e1-1-3-1		
e1-1-3-2		
e1-1-3-3		
e1-1-3-4		

Edit E1...      Edit V5 Link...      Remove V5 Link

Close

**Figure 5-7 "IO\_E1" Window**

This window can be displayed even when the plug-in is not inserted.



The following table shows the view/edit options of the *IO\_E1* window:

Parameters/ Buttons	Description
<b>NE Name</b>	NE name of the selected NE (max. 30 characters).
<b>Slot</b>	<p>Slot format: ioe1-shelf number-slot for working IO_E1s and ioe1p-shelf number for the protection IO_E1 (protection of IO_E1 is not yet implemented for R1.3).</p> <p>Possible values: ioe1-{1}-{1,4} for working IO_E1 ioe1p-{1} for protection IO_E1 (not yet implemented).</p>
<b>Inventory Information</b>	<p>The following fields will be empty, if no plug-in is inserted. Otherwise the read-only text fields provide the following information:</p> <p><b>Card Type:</b> 11-character mnemonic used to identify the general type of function provided. Possible value: IO_E1.</p> <p><b>Serial Number:</b> 12-character alphanumeric code that includes the date and place of manufacture.</p> <p><b>Apparatus Code:</b> Specifies the function of the plug-in. Possible value: FAC500.</p> <p><b>ICC (InterChangeability Code):</b> Indicates the interchangeability among plug-ins to specify forward/backward compatibility. Format of the ICC is <b>m:n</b> where <b>m</b> is the issue number and <b>n</b> the series number.</p> <p><b>CLEI:</b> Not applicable.</p> <p><b>ECI:</b> Not applicable.</p>
<b>E1 Information</b>	<p>The information in this field is displayed in a table (3 rows, one per E1):</p> <ul style="list-style-type: none"> <li>■ <b>Feeder:</b> Physical address of the E1 feeders. Format: e1-shelf-slot-port (e.g. e1-1-1-4). Possible Values: e1-1-{1, 4} -{1, 4}.</li> <li>■ <b>V5 Interface id:</b> The V5 Interface id is displayed (if present). In case of leased lines, this field shows "Leased".</li> <li>■ <b>V5 Link id:</b> The id used to identify the V5 Links. Format: {0, 255}. In case of leased lines, this field shows "Leased".</li> </ul>

Parameters/ Buttons	Description
	<p>The following buttons are available only if a row in the feeder list has been selected and the feeder is not used for leased lines.</p> <p>The <b>Edit E1...</b> button provides access to the <i>E1 Feeder/V5 Link</i> window (tab E1 Feeder) where you will be able to edit the E1 feeder parameters.</p> <p>The <b>Label...</b> button provides access to the <i>E1 Feeder/V5 Link</i> window (tab V5 Link Table) to add/edit V5 Link parameters.</p> <ul style="list-style-type: none"> <li>■ If the selected E1 feeder is associated to a V5 Link the label is <b>Edit V5 Link...</b></li> <li>■ If the selected E1 feeder is not associated to a V5 Link the label is <b>Add V5 Link...</b></li> </ul> <p>The <b>Remove V5 Link</b> button can be used to delete E1 feeder to V5 Link association. If the feeder is used for leased lines, this button is not available.</p>

If you want to ...	then ...
edit a E1 parameter	select the desired row in the <b>E1 Information</b> list and press <b>Edit E1...</b> or double click on the row. The <i>E1 Feeder/V5 Link</i> window (tab E1 Feeder) pops up (cf. Chapter 5.3.2.1.2, page 5-29).
edit a V5 Link	select the appropriate row in the <b>E1 Information</b> list and press <b>Edit V5 Link...</b> The <i>E1 Feeder/V5 Link</i> window (tab V5 Link) pops up (cf. Chapter 5.4.2.4.2, page 5-104).
add a V5 Link	select the appropriate row in the <b>E1 Information</b> list and press <b>Add V5 Link...</b> The <i>E1 Feeder/V5 Link</i> window (tab Cross-Connection) pops up (cf. Chapter 5.4.2.4.2, page 5-104).
delete a V5 Link	select the appropriate row in the <b>E1 Information</b> list and press <b>Remove V5 Link...</b> A <i>Warning</i> window pops up displaying the following message:

Removing V5 Link id may be service affecting. Do you want to continue?

If you decide to continue, the remove operation will be started.

### 5.3.2.1.2 Edit E1 Feeder

Complete the following procedure to edit the E1 feeder data:

Step	Procedure
------	-----------


- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE -&gt; Shelf -&gt; FAC500 -&gt; E1 Feeder</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> via the menu bar. The <i>E1 Feeder/V5 Link</i> window (tab E1Feeder) pops up. |
|----|---|

This window can also be reached from the *IO\_E1* window (cf. Chapter 5.3.2.1.1, page 5-26) or *E1 Feeder List* window (cf. Chapter 5.4.2.3, page 5-99) by clicking on **Edit E1....**

The screenshot shows the 'E1 Feeder/V5 Link' window with the 'Physical Feeder' tab selected. The 'NE Name' field contains 'TCI\_LNF14'. Below it, the 'Physical Feeder' field contains 'e1-1-4-2'. The 'V5 Link id' field is empty. The 'Impedance' field is empty, with a 'Get' button to its right. The 'Loopback' field contains 'Clear', with a 'Set' button to its right. The 'Timing Source Reference' field contains 'No', with an 'Edit...' button to its right. Below these fields is a 'Service State' section with an 'Operational State' field and a 'Get' button. At the bottom of the window are 'Cancel', 'Apply', and 'Close' buttons. A red 'X' button is visible in the bottom right corner of the window frame.

**Figure 5-8 "E1 Feeder/V5 Link" Window (Tab Physical Feeder)**

The following table shows the view/edit options of the physical feeder parameters:

Parameters/ Buttons	Description
<b>E1 Feeder Data</b>	<p><b>Physical Feeder:</b> This option menu is used to select the specific E1 feeder the user wants to display the information for. The selection is also valid for the V5 Link tab. The list shows all E1 feeders present in the shelf.</p> <p>Format: e1-shelf-slot-feeder. Possible values: e1-1-{1, 4}-{1, 4}.</p> <p><b>V5 Link id:</b> This field is only empty when the E1 feeder is not associated to a V5 link or a leased line service.</p> <p>Possible values: {0, 255}.</p> <p>If the E1 feeder is associated to a V5 link the V5 link id is shown in this field.</p> <p>If the feeder is related to a leased line link the value "Leased" is shown.</p> <p><b>Impedance:</b> Displays the impedance of the E1 feeder termination.</p> <p>Possible values: 120 Ohm, 75 Ohm.</p> <p><b>Get:</b> This button can be used to get the E1 impedance from the NE.</p> <p><b>Loopback:</b> This field displays the current loopback state (<b>Clear</b> or <b>Set</b>). This state can be modified via the <b>Label</b> button on the right hand side.</p> <p><b>Label:</b> This button can be used to set or to clear the E1 loopback. Depending on the current state, this button displays the possible operation (<b>Clear</b>, if the loopback state is <b>Set</b> and <b>Set</b> if the loopback is <b>Clear</b>).</p> <p> <b>NOTE:</b> This button is disabled if the E1 feeder is used as timing source reference (see below).</p> <p><b>Timing Source Reference:</b> Indicates whether the selected E1 is the timing source reference or not. This reference can only be changed via the <b>Edit...</b> button on the right hand side (see below).</p> <p>Possible values: Yes, No.</p> <p><b>Edit...:</b> This button provides access to the <i>NE Information</i> window (Timing Source Control tab - cf. Chapter 5.3.3.3, page 5-52) to modify the current NE timing source reference.</p>

Parameters/ Buttons	Description
<b>Operational State</b>	<b>Service State:</b> Shows the current service state of the NE. Possible values: Enabled, Disabled.  <b>Get:</b> This button can be used to get the current service state from the NE.

2. Use the option menu **Physical Feeder** to select an appropriate E1 feeder.
3. Press the **Label** button to define the loopback state.
4. Click on **Apply** to confirm the changes.

If the loopback state has been changed to "Set" a *Warning* window pops up:

`setting Loopback for a feeder can be service  
affecting. Do you want to continue?`

5. Enter **Yes** to confirm (or **No** to reject).

Select tab **V5 Link** (cf. next section) or click on **Close** to exit the window.

### 5.3.2.1.3 Configure a COMDAC

The COMDAC (Common Data and Control) plug-in performs the main bandwidth management and control functions for the system.

#### Procedure

Complete the following procedure to view/edit the COMDAC data:

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; Shelf -&gt; COM500</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> via the menu bar or single click on the plug-in <b>COMDAC</b> in <i>Shelf View</i> window. The <i>COMDAC</i> window pops up.

**Figure 5-9 "COMDAC" Window**

This window contains all the information related to the COMDAC. It can be displayed even when the plug-in is not inserted.

The following table shows the view/edit options of the *COMDAC* window:

Parameters/ Buttons	Description
<b>NE Name</b>	NE name of the selected NE (max. 30 characters).
<b>Slot</b>	Slot number where the COMDAC is plugged in. Slot format: comdac-1-{1,2}
<b>Inventory Information</b>	<p>The following fields will be empty, if no plug-in is inserted. Otherwise the read-only text fields provide the following information:</p> <p><b>Card Type:</b> 11-character mnemonic used to identify the general type of function provided. Possible value: COMDAC.</p> <p><b>Serial Number:</b> 12-character alphanumeric code that includes the date and place of manufacture.</p> <p><b>Apparatus Code:</b> Specifies the function of the plug-in. Possible value: COM100.</p> <p><b>ICC (InterChangeability Code):</b> Indicates the interchangeability among plug-ins to specify forward/backward compatibility. Format of the ICC is <b>m:n</b> where <b>m</b> is the issue number and <b>n</b> the series number.</p> <p><b>CLEI:</b> Code assigned by Bellcore that provides information about the functionality of the plug-in.</p> <p><b>ECI:</b> Code that corresponds to the bar-coded label on the faceplate of the plug-in. There is a one-to-one correspondence between CLEI and ECI codes.</p> <p><b>SW Version:</b> Obtained from the NE at connection time. Internally, the AEM-NB will have to verify whether the mentioned SW Version is manageable by the system.</p> <p><b>Program Code:</b> Code of the SW currently stored in the plug-in.</p>
<b>Operation &amp; Protection</b>	This field is described in Chapter 5.3.3.6, page 5-58.
<b>Ongoing Tasks</b>	These check boxes indicate operations in progress which can take a long time and must be known by the operator. They will be refreshed when the window is launched or when refreshing the whole window.

### 5.3.2.1.4 Configure a CIU

The CIU (Communication Interface Unit) plug-in provides access for circuit and drop testing and craft access functions.

#### Procedure

Complete the following procedure to view the CIU data:

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; Shelf -&gt; DTP500</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> via the menu bar or single click on the plug-in <b>CIU</b> in <i>Shelf View</i> window. The <i>CIU</i> window pops up:

The screenshot shows a window titled "CIU". It contains the following fields:

- NE Name: TCL-NE12
- Slot: ciu-1
- Inventory Information section:
  - Card Type: CIU
  - Serial Number: 98OC06110591
  - Apparatus Code: DTP500
  - ICC: 1-2
  - CLEI: (empty)
  - ECI: (empty)
- A "Close" button at the bottom center.
- A red "X" button in the bottom right corner.

**Figure 5-10 "CIU" Window**

This window contains all information related to the CIU. It can be displayed even when the plug-in is not inserted.

The following table shows the view/edit options of the *CIU* window:

Parameters/ Buttons	Description
<b>NE Name</b>	NE name of the selected NE (max. 30 characters).
<b>Slot</b>	Slot number where the CIU is plugged in.



Parameters/ Buttons	Description
<b>Inventory Information</b>	<p>The following fields will be empty, if no plug-in is inserted. Otherwise the read-only text fields provide the following information:</p> <p><b>Card Type:</b> 11-character mnemonic used to identify the general type of function provided. Possible value: CIU.</p> <p><b>Serial Number:</b> 12-character alphanumeric code that includes the date and place of manufacture.</p> <p><b>Apparatus Code:</b> Specifies the function of the plug-in. Possible value: DTP500.</p> <p><b>ICC (InterChangeability Code):</b> Indicates the interchangeability among plug-ins to specify forward/backward compatibility. Format of the ICC is <b>m:n</b> where <b>m</b> is the issue number and <b>n</b> the series number.</p> <p><b>CLEI:</b> Not applicable.</p> <p><b>ECI:</b> Not applicable.</p>

### 5.3.2.1.5 Configure an IO\_HDLC

The IO\_HDLC (High-Level Data Link Control) plug-in primarily performs a frame relay function of D-channel messages between the ISDN subscribers connected to a NE and the V5 communication channels.

#### Procedure

Complete the following procedure to view/edit the IO\_HDLC data:

Step	Procedure
------	-----------

- |    |  |
|----|--|
| 1. | <p>Select <b>All -&gt; NE -&gt; Shelf -&gt; IDC500</b> in the Network Browser and <b>Edit</b> via the cursor menu</p> <p>or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> via the menu bar</p> <p>or single click on the plug-in <b>IO_HDLC</b> in <i>Shelf View</i> window.</p> <p>The <b>IO_HDLC</b> window pops up:</p> |
|----|--|

**Figure 5-11 "IO\_HDLC" Window**

This window contains all information related to the IO\_HDLC. It includes hardware and software data (inventory) as well as operational and protection state. It can be displayed even when the plug-in is not inserted.

The following table shows the view/edit options of the *IO\_HDLC* window:

Parameters/ Buttons	Description
<b>NE Name</b>	NE name of the selected NE (max. 30 characters).
<b>Slot</b>	Slot number where the IO_HDLC is plugged in. Slot format: io-hdlc{1,2}.
<b>Inventory Information</b>	<p>The following fields will be empty, if no plug-in is provisioned. Otherwise the read-only text fields provide the following information:</p> <p><b>Card Type:</b> 11-character mnemonic used to identify the general type of function provided. Possible value: IO_HDLC.</p> <p><b>Serial Number:</b> 12-character alphanumeric code that includes the date and place of manufacture.</p> <p><b>Apparatus Code:</b> Specifies the function of the plug-in. Possible value: IDC500.</p> <p><b>ICC (InterChangeability Code):</b> Indicates the interchangeability among plug-ins to specify forward/backward compatibility. Format of the ICC is <b>m:n</b> where <b>m</b> is the issue number and <b>n</b> the series number.</p> <p><b>CLEI:</b> Not applicable.</p> <p><b>ECI:</b> Not applicable.</p>
<b>Provisioning Info</b>	<p>The option menu <b>Provisioned Apparatus Code</b> can be used to see and change the slot provisioning info. If nothing is provisioned, this field displays "None". Otherwise it displays the provisioned card type.</p> <p>Possible values: None and IDC500.</p>
<b>Operation &amp; Protection</b>	<p><b>Administration State:</b> This option menu is used to see and select the administrative state for the IO_HDLC.</p> <p>Possible values are: Locked and Unlocked. After creation, the default value is unlocked.</p> <p><b>Protection State</b> shows whether the selected IO_HDLC is working or not.</p> <p>Possible values: Working, Standby and Not Applicable (protection mode is disabled).</p> <p>The <b>HDLC Protection...</b> button provides access to the <i>Shelf Protection</i> window (tab IO_HDLC) to allow you to modify the protection scheme or to perform protection switching.</p>
<b>Apply</b>	This button is used to confirm the changes. It is available only when some changes have been made on the window (i.e. change in <b>Provisioned Apparatus Code</b> or <b>Administrative State</b> ).

If you want to ...	then ...
change the provisioned card type	use the option menu <b>Provisioned Card Type</b> and click on <b>Apply</b> .
modify the protection scheme	press <b>HDLC Protection....</b> The <i>Shelf Protection</i> window pops up (cf. Chapter 5.3.3.7.2, page 5-63).
change the administrative state	use the option menu <b>Administration State</b> and click on <b>Apply</b> . When changing from Unlocked to Locked a <i>Warning</i> window pops up displaying the following message:

Changing the IO-HDLC administrative state to Locked may be service affecting in mixed (POTS/ISDN) system configurations if no protection switch is possible. Do you want to continue?

If you decide to continue, the change operation will be started.

### 5.3.2.1.6 Configure an Application Pack

The APs (Application Packs) provide the line side interface functionality that provide service to end-users.

#### Background

The *AnyMedia* Access System R1.3 uses a provisioning model to provide service, i.e. the AP must be pre-provisioned by defining its function and setting the required options. For example, a POTS AP has to be pre-provisioned first to create a POTS or ALL service for a subscriber. Should the physical inventory change, i.e. if an AP is plugged or removed, any changes in the inventory database will be notified automatically to the *AnyMedia* Access System.

AP provisioning will be performed to establish a desired POTS plug-in type in a desired slot xx. To be fully functional/operational, an AP must both be inserted and provisioned. In addition, the provisioned AP must match the actual type of the inserted plug-in. An AP can be provisioned and configured by the AEM-NB even if the slot is still empty.

#### Procedure

Complete the following procedure to view/edit the AP data:

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE -&gt; Shelf -&gt; LPZ100 (LPP100, LPU112, TAP100)</b> <sup>1</sup> in the Network Browser and <b>Edit</b> via the cursor menu<br>or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> via the menu bar<br>or single click on the <b>AP</b> in <i>Shelf View</i> window.<br>The <i>Application Pack</i> window pops up. |
|----|---|



#### NOTE:

The window shown here as an example belongs to a provisioned application pack. The window for a not provisioned application pack would not display the **Drop Information** region.

1

If the selected slot is not yet provisioned the slot id will be shown instead of the apparatus code.

The screenshot shows the 'Application Pack' window with the following fields and sections:

- NE Name:** TCL-NE14
- Slot:** ap-1-8
- Inventory Information:**
  - Card Type:** (empty)
  - Serial Number:** 99OC01413232
  - Apparatus Code:** LPZ100B
  - ICC:** 3-4
  - CLEI:** E5ALCPUBAA
  - ECI:** 238520
- Provisioning Info:**
  - Provisioned Apparatus Code:** LPZ100
- Drop Info:**

Drop	V5 Interface id	User Port Address	User Port Type
drop-1-8-1			
drop-1-8-2			
drop-1-8-3			
drop-1-8-4			
drop-1-8-5			
drop-1-8-6			
drop-1-8-7			
drop-1-8-8			
drop-1-8-9			

Buttons at the bottom: Add V5 User Port, Edit V5 User Port, Remove V5 User Port, Apply, Close.

**Figure 5-12 "Application Pack" Window**

This window contains all information related to the AP. It can be displayed even when the plug-in is not inserted.

The following table shows the view/edit options of this window:

Parameters/ Buttons	Description
<b>NE Name</b>	NE Name of the selected NE (max. 30 characters).
<b>Slot</b>	Slot number where the AP is plugged in. Format: ap-{1,16}

Parameters/ Buttons	Description
<b>Inventory Information</b>	<p>The following fields will be empty, if no plug-in is provisioned. Otherwise the read-only text fields provide the following information:</p> <p><b>Card Type:</b> Not applicable.</p> <p><b>Serial Number:</b> 12-character alphanumeric code that includes the date and place of manufacture.</p> <p><b>Apparatus Code:</b> Specifies the function of the plug-in. Possible values: LPZ100B, LPP100B, LPU112, TAP100, LPA910, LPA400, LPA900.</p> <p><b>ICC (InterChangeability Code):</b> Indicates the interchangeability among plug-ins to specify forward/backward compatibility. Format of the ICC is <b>m:n</b> where <b>m</b> is the issue number and <b>n</b> the series number.</p> <p><b>CLEI:</b> Code assigned by Bellcore that provides information about the functionality of the plug-in.</p> <p><b>ECI:</b> Code that corresponds to the bar-coded label on the face-plate of the plug-in. There is a one-to-one correspondence between CLEI and ECI codes.</p>
<b>Provisioning Info</b>	<p>This option menu <b>Provisioned Apparatus Code</b> shows the APs available for the NE release. If no AP is yet provisioned <b>None</b> is displayed.</p> <p>Possible values: None or LPZ100, LPP100, LPZ120, LPU112 and TAP100.</p> <p>⇒ <b>NOTE:</b> The <b>Provisioned Apparatus Code</b> may be different from the <b>Apparatus Code</b> shown in the Inventory Information field. The <b>Apparatus Code</b> is related to a certain card (e.g. LPZ100B) whereas the <b>Provisioned Apparatus Code</b> is related to a family of cards (e.g. LPZ100).</p> <p>⇒ <b>NOTE:</b> Broadband packs (LPA910, LPA400, LPA900) cannot be provisioned via this interface, broadband packs are not included in this list.</p>

Parameters/ Buttons	Description
<b>Drop Information</b>	<p>This pane contains a table displaying drop information.</p> <p>It exist only if the <b>Provisioned Apparatus Code</b> is one of the following: LPZ100, LPP100, LPU112, TAP100.</p> <p>This information is presented in a 4-column table. The table is sorted by <b>Drop</b>. A scroll bar allows navigation through the table. Rows in the table can be selected to add or edit (single row selection) or remove (single or multiple row selection) the corresponding user port(s) through the use of the <b>Add V5 User Port...</b>, <b>Edit V5 User Port...</b> or <b>Remove V5 User Port...</b> buttons (see below).</p> <ul style="list-style-type: none"> <li>■ <b>Physical Drop:</b> Identifies the drop within the AP. Format: drop-shelf-slot-port Possible values: drop-1-{1,16}-{1, 32}</li> </ul> <p>The following entries are available only if a port is already cross-connected.</p> <ul style="list-style-type: none"> <li>■ <b>V5 Interface id:</b> Shows the V5 Interface id on which the service is provided. Possible values: {0, 16777215} If the drop is used for leased lines "Leased" is displayed.</li> <li>■ <b>V5 User Port Address:</b> Indicates the id within the layer 3 (PSTN port) or Envelope Function Address (ISDN-BRA port) of the subscriber (only available if the subscriber is cross-connected to a V5 Interface). Possible values: {1, 32767} for PSTN                           {0, 8175} for ISDN-BRA If the drop is used for leased lines "Leased" is displayed.</li> <li>■ <b>V5 User Port Type:</b> Shows the type of service provided. Possible values: PSTN, ISDN-BRA or Leased. PSTN and ISDN-BRA are not possible in the same application pack. If the drop is used for leased lines "Leased" is displayed.</li> </ul>



Parameters/ Buttons	Description
	<p>The <b>Add V5 User Port...</b> button is not available for leased lines. Otherwise it provides access to the <i>V5 PSTN User Port</i> or <i>V5 ISDN-BRA User Port</i> window, depending on the type of <b>Apparatus Code</b>. In this case, the drop will be transferred. This option is only available if the selected drop is not yet cross-connected.</p> <p>Access to the <i>V5 PSTN User Port</i> window for the following apparatus codes: LPZ100, LPP100, LPZ120.</p> <p>Access to the <i>V5 ISDN-BRA User Port</i> window for the apparatus code LPU112.</p> <p>The <b>Edit V5 User Port...</b> button provides access to the <i>V5 PSTN User Port</i> or <i>V5 ISDN-BRA User Port</i> window, depending on the service being provided by the selected drop. There you will be able to edit the user port parameters. This option is only available if the selected drop is already cross-connected.</p> <p>The <b>Remove V5 User Port...</b> button removes the cross-connection selected in the list (see above). This option is only available if the drop is already cross-connected and providing non-leased service.</p>
<b>Apply</b>	This button is available only if the <b>Provisioned Apparatus Code</b> has been modified.

2. Use the option menu **Provisioned Apparatus Code** to select the appropriate AP.

3. Press **Apply** to confirm (the window remains on screen for further use).

If you want to ...	then ...
add a V5 User Port	press <b>Add V5 User Port....</b> The <i>V5 PSTN User Port</i> or <i>V5 ISDN-BRA User Port</i> window pops up (cf. Chapter 5.4.5.1, page 5-118 for PSTN and Chapter 5.4.5.2, page 5-124 for ISDN-BRA).
edit a V5 User Port	select a row in the <b>Drop Information</b> list and press <b>Edit V5 User Port....</b> The <i>V5 PSTN User Port</i> or <i>V5 ISDN-BRA User Port</i> window pops up (cf. Chapter 5.4.5.1, page 5-118 for PSTN and Chapter 5.4.5.2, page 5-124 for ISDN-BRA).
delete a cross-connection	select the desired <b>User Port Address</b> in the <b>Drop Information List</b> and press <b>Remove V5 User Port....</b> A <i>Warning</i> window pops up displaying the following message.

**Removing V5 User Port may be service affecting. Do you want to continue?**

4. If you decide to continue, the remove operation will be started. The information displayed will be updated once the remove operation is finished to show the current list.

### 5.3.3 Edit/View of Configuration Data

All edit/view actions of configuration data can be started via *NE Name Information* window.

#### NE Name Information

**Figure 5-13 "NE Name Information" Window**

This window includes of 5 tabs:

- NE Details (cf. Chapter 5.3.1, page 5-17)
- NE Synchronization (cf. Chapter 5.3.3.1, page 5-45)
- NE Inventory Data (cf. Chapter 5.3.3.2, page 5-49)
- Timing Source Control (cf. Chapter 5.3.3.3, page 5-52)
- Date & Time (cf. Chapter 5.3.3.4, page 5-56).

#### 5.3.3.1 Network Element Synchronization

##### 5.3.3.1.1 Configuration Information Synchronization

#### Overview

The possibility exists for the AEM-NB database to become inconsistent with the information stored locally in the NE (Non-Volatile Data Storage). A database re-synchronization capability provides a mechanism for the AEM-NB database to be made consistent (synchronized) with the locally stored NE information.

Two NE configuration data synchronization states can be identified:

- **SYNC:** The AEM-NB database is consistent with the locally stored NE information and all the autonomous messages concerning configuration changes are enabled (DB changes, switch reports and some events of type protection switches, lockout and loop back).
- **ASYNC:** The AEM-NB database and the NE configuration data are out of synchronization and/or configuration reports are inhibited and/or AEM-NB configuration message buffer is overflowing.

For more information refer to the NE documentation for R1.3.

#### 5.3.3.1.2 Alarm Information Synchronization

##### Overview

In general alarms can be considered independently of each other (any alarm report can be processed by the AEM-NB independent of other alarm reports). The AEM-NB distinguishes two possible states for alarm handling: alarms from NEs are enabled or they are inhibited.

Two NE alarm processing states can be considered:

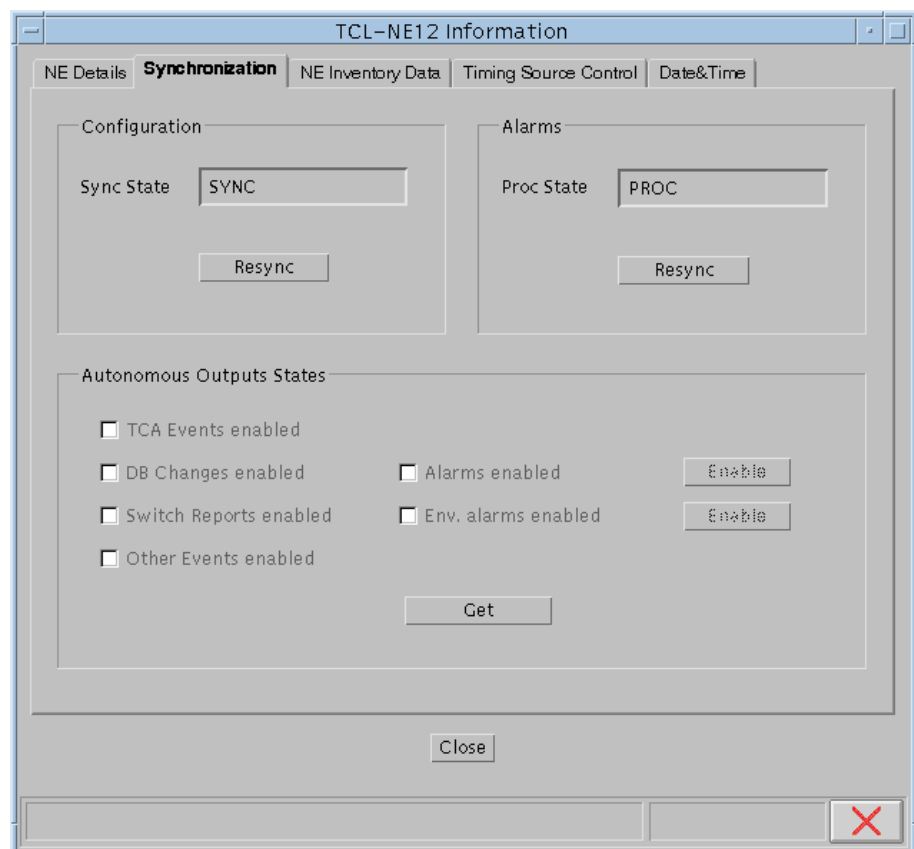
- **PROC:** The AEM-NB alarm database is consistent with the current NE alarms and alarm and environment alarm reports are enabled.
- **BLOCK:** The AEM-NB alarm database and the current NE alarms are out of synchronization due to alarm buffer overflow. The AEM-NB alarm database is only a snapshot of NE alarm information at a certain moment in time.

For more information refer to the NE documentation for R1.3.

**Parameter Setting**

Complete the following procedure to modify the synchronization states for configuration and alarms and to define the autonomous output states:

- | Step | Procedure   |
|------|---|
| 1.   | Select <b>All -&gt; NE</b> in the Network Browser and <b>NE Information</b> via the cursor menu<br>or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> or <b>Equipment -&gt; EM-NE Synchronization</b> via the menu bar.<br>The <i>NE Name Information</i> window pops up. |
| 2.   | Click on tab <b>Synchronization</b> .<br>(this step is not necessary if the <i>NE Name Information</i> window has been opened via <b>Equipment -&gt; EM-NE Synchronization</b> ).   |



**Figure 5-14 "NE Name Information" Window (Tab Synchronization)**

The following table shows the view/edit options of the *NE Name Information* window (tab Synchronization):

Parameters/ Buttons	Description
<b>Configuration</b>	The <b>Sync State</b> represents the configuration synchronization state between the AEM-NB and NE. This information is obtained from the NE and it will be automatically updated. Possible values are: SYNC and ASYNC.
<b>Alarms</b>	The <b>Proc State</b> represents the alarm processing state between the AEM-NB and NE. This information is obtained from the NE and it will be automatically updated. Possible values are: PROC and BLOCK.
<b>Autonomous Outputs States</b>	<p>The check boxes can be used to show and edit autonomous output states. They are enabled only after clicking on the <b>Get</b> button.</p> <p>The <b>Get</b> button can be used to show the current autonomous output states of the NE.</p>

3. Use the **Label** button in the pane **Configuration** to change the **Sync State**.  
If the **Sync State** is SYNC, the label says **Resync**. If the **Sync State** is ASYNC, the label says **Sync**.
4. Use the **Resync** button in the pane **Alarms** to re-synchronize the alarm processing state.
5. Click on the **Get** button to update the display of the autonomous output states.
6. Use the check boxes to change the autonomous output states **Alarms** and/or **Env. alarms** (disabled - check mark, enabled - clear).
7. Click on another tab to change the window or click on **Close** to exit the window.

### 5.3.3.2 Network Element Inventory Data

This window provides NE inventory data.

#### Procedure

Complete the following procedure to get the inventory data:

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE</b> in the Network Browser and <b>NE Information</b> via the cursor menu<br>or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> or <b>Equipment -&gt; NE Inventory Data</b> via the menu bar.<br>The <b>NE Name Information</b> window pops up. |
| 2. | Click on tab <b>NE Inventory Data</b> .<br>(this step is not necessary if the <b>NE Name Information</b> window has been opened via <b>Equipment -&gt; NE Inventory Data</b> ).   |

The screenshot shows the 'TCL-NE12 Information' window with the 'NE Inventory Data' tab selected. The window contains two tables:

**NE Inventory Table:**

Shelf/Slot	Circuit Pa...	Apparatus...	Serial Nu...	ECI	CLEI	ICC	Sw
sh-1/ioe1...	IOE1	FAC500	99OC021...			1-2	
sh-1/ioe1...	IOE1	FAC500	99OC011...			1-2	
sh-1/ioe1...	IOE1	FAC500	99OC021...			1-2	
sh-1/ciu-1	CIU	DTP500	98OC061...			1-2	
sh-1/com...	COMDAC	COM100	98OC042...	228863	SLC1CG0...	1-1	01
sh-1/	AnyMedia...						
sh-1/com...							
sh-1/ie1...							
sh-1/ie1...							
sh-1/ap...							
sh-1/ap...							
sh-1/ap...							

**Summary Table:**

Apparatus Code	Number of Units
COM100	1
DTP500	1
Unknown	21
FAC500	3

**Figure 5-15 "NE Name Information" Window (Tab NE Inventory Data)**

Two non-editable tables display NE inventory information. The first table contains per slot data, while the second one provides summarized information per card type.

Parameters/ Buttons	Description
<b>NE Inventory data</b>	<p>Depending on the card some of the following fields are not available.</p> <p><b>Shelf/Slot:</b> Numeric field that identifies the position of each plug-in.</p> <p><b>Circuit Pack Type:</b> Mnemonic that identifies the plug-in type.</p> <p>Possible values: COMDAC, CIU, IO_E1, IO_HDLC, PROG2W, COIN, ZEUS, ISDN12_U, TAP, AFM_E3 and ADSL4.</p> <p><b>Apparatus Code:</b> Identifies the specific function provided by the plug-in unit.</p> <p>Possible values: COM500, DTP500, FAC500, IDC500, LPZ100, LPP100, LPZ120, LPU112, TAP100, LPA910, LPA900, LPA400.</p> <p><b>Serial Number:</b> A 12-character alphanumeric code that identifies each plug-in. It includes the date and place of manufacture.</p> <p><b>ECI:</b> Code that corresponds to the bar-coded label on the face-plate of the plug-in. There is a one-to-one correspondence between CLEI and ECI codes.</p> <p>⇒ <b>NOTE:</b> This field is empty for IO_E1 and IO_HDLC.</p> <p><b>CLEI:</b> Code assigned by Bellcore that provides information about the functionality of the plug-in.</p> <p>⇒ <b>NOTE:</b> This field is empty for IO_E1 and IO_HDLC.</p> <p><b>ICC:</b> Indicates the interchangeability among plug-ins to specify forward/backward compatibility. Format of the ICC is <b>m:n</b> where <b>m</b> is the issue number and <b>n</b> the series number.</p> <p><b>SW Version:</b> Obtained from the NE at connection time. Internally, the AEM-NB will have to verify whether the mentioned SW Version is manageable by the system. Only applicable to the COMDACs or the shelves, where the shelf-back-plane version will be displayed.</p> <p><b>Program Equipment Code:</b> Code of the SW currently stored in the plug-in. Only applicable to the COMDAC.</p>



Parameters/ Buttons	Description
Summary	<p><b>Circuit Pack Type:</b> Displays a mnemonic that identifies the plug-in type.</p> <p>Possible values are: COMDAC, CIU, IO_E1, IO_HDLC, PROG2W, COIN, ZEUS, ISDN12_U, TAP, AFM_E3, ADSL4 and AFM_DS3.</p> <p><b>Number of Units:</b> Displays two numbers: the number of inserted plug-ins and the number of not inserted plug-ins.</p>

3. Click on another tab to change the window or click on **Close** button to exit the window.

### 5.3.3.3 Configuration of Timing Source

#### Overview

The *AnyMedia* Access System supports two timing modes<sup>1</sup>: Free Running and Loop Timed.

- **Free Running Mode:** For free-running operation, the NE derives timing from an internal crystal oscillator (XO) with an accuracy not worse than  $\pm 32$  parts-per-million (ppm) over full power supply, temperature, and life-time. The free-running mode is intended only for turn-up and failure conditions.
- **Loop Timed Mode:** In this mode the NE recovers the clock from one of the up to 16 feeder E1 interfaces or from a Station Clock Interface (SCI).

#### Timing Inputs

The two timing inputs are identified as **Primary** (Reference Source) and **Secondary** (Protection Source). The first E1 feeder of the first IO\_E1 plug-in is the default primary input, and the first feeder of the second IO\_E1 plug-in is the default secondary input. The network provider can tailor the set of valid timing inputs and their priorities via provisioning. The Primary and Secondary reference signals can be selected from any physical feeder inputs on any two IO\_E1 plug-ins, or from two feeder inputs on the same plug-in. The NE can continue to derive timing from the reference inputs if one or both of the physical inputs is (are) switched to the protection IO\_E1 plug-in.

For more information refer to the NE documentation for R1.3.

Upon initialization, the NE selects the primary input as the active reference, and the secondary input as its alternate source. If the primary reference fails, the NE hardware switches to the alternate source, providing synchronization reference source protection is available (cf. Chapter 5.3.3.7, page 5-59).

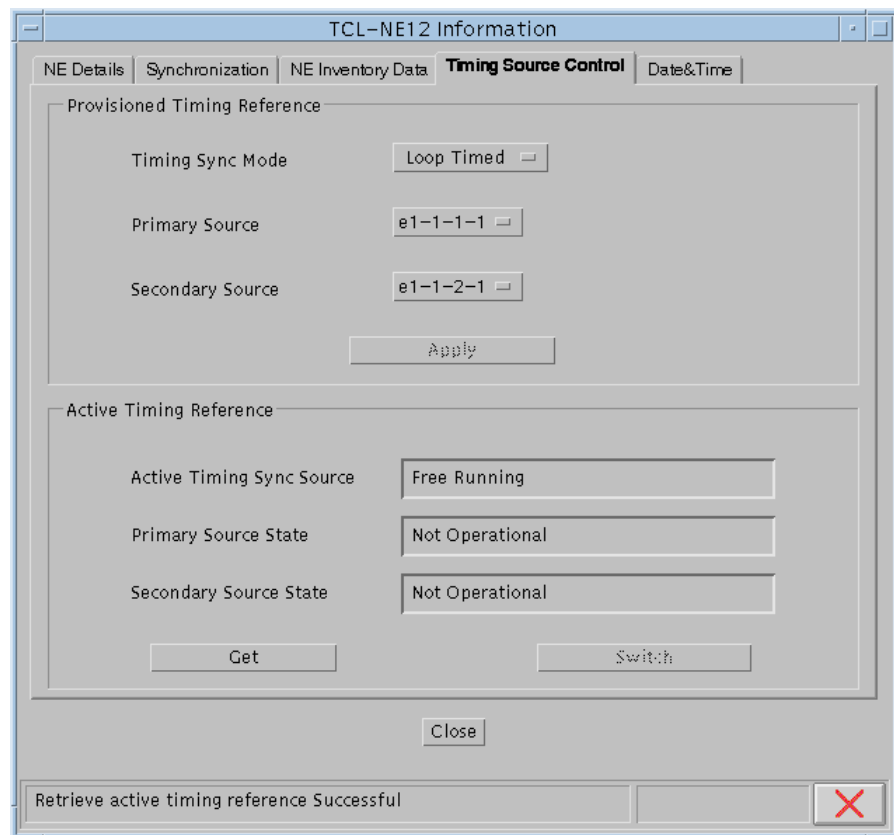
#### Procedure

Complete the following procedure to configure the timing source:

Step	Procedure
1.	Select the <b>All -&gt; NE</b> in the Network Browser and <b>NE Information</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> or <b>Equipment -&gt; Provisioning -&gt; Timing Source Control</b> via the menu bar. The <i>NE Name Information</i> window pops up.
2.	Click on tab <b>Timing Source Control</b> . (this step is not necessary if the <i>NE Name Information</i> window has been opened via <b>Equipment -&gt; Provisioning -&gt; Timing Source Control</b> ).

1

The *AnyMedia* Access System hardware also supports external timing via a composite office clock; however, this mode is not supported in the release software.



**Figure 5-16 "NE Name Information" Window (Tab Timing Source Control)**

This window provides the user with the facilities needed to configure the NE timing source. The following table shows the view/edit options of the *Timing Source Control* window:

Parameters/ Buttons	Description
<b>Provisioned Timing Reference</b>	<p><b>Timing Sync Mode: Free Running or Loop Timed.</b> Only in case of <b>Loop Timed</b> the next two fields (<b>Primary Source</b> and <b>Secondary Source</b>) are available.</p> <p><b>Primary Source:</b> If <b>Timing Sync Mode</b> is <b>Loop Timed</b>, the primary source (working) and (optionally) the secondary source (standby) can be selected.</p> <p>Possible values: any of the available feeders (e1-1-{1, 4}-{1, 4}) or station clock.</p> <p>Once the source(s) of synchronization has been selected, click on the <b>Apply</b> button.</p> <p><b>Secondary Source:</b> If <b>Timing Sync Mode</b> is <b>Loop Timed</b> and <b>Primary Source</b> has been selected, the secondary source can be selected as a protection timing synchronization source if the primary source fails.</p> <p>Possible values: any of the available feeders (e1-1-{1, 4}-{1, 4}) or station clock.</p> <p>Once the protection source of synchronization has been selected, click on the <b>Apply</b> button.</p> <p>⇒ <b>NOTE:</b> The secondary source must be different from the primary source. Otherwise there is no protection available.</p> <p>The <b>Apply</b> button is available only if:</p> <ul style="list-style-type: none"> <li>■ <b>Timing Sync Mode</b> has been changed.</li> <li>■ <b>Synchronization Mode</b> is <b>Loop Timed</b> and at least one source has been modified.</li> </ul> <p>⇒ <b>NOTE:</b> During the apply operation, the <b>Get</b> and <b>Switch</b> buttons are disabled. The whole subpane will be updated as result of the operation.</p>

Parameters/ Buttons	Description
<b>Active Timing Reference</b>	<p>If the <b>Get</b> button has not been pressed the following fields are empty.</p> <p><b>Active Timing Sync Source:</b> Shows the active timing sync source of the NE.</p> <p>Possible values: Free Running, Loop Timed / PRI and Loop Timed / SEC.</p> <p><b>Primary Source State:</b> Shows the primary source operational state.</p> <p>Possible Values are: Operational, Not Operational and empty field (no value received).</p> <p><b>Secondary Source State:</b> Shows the secondary source operational state.</p> <p>Possible Values are: Operational, Not Operational and empty field (no value received).</p> <p>The <b>Get</b> button can be used to retrieve the <b>Active Timing Synchronization Source</b> and the operational state of primary and secondary sources (if applicable) from the NE.</p> <p>⇒ <b>NOTE:</b> During the get operation, the <b>Apply</b> and <b>Switch</b> buttons are disabled. The provisioned timing reference subpane will also be updated as result of this operation.</p> <p>The <b>Switch</b> button is enabled only if the <b>Active Timing Synchronization Source</b> is not <b>Free Running</b> and the operational state of the reference source is <b>Operational</b>.</p> <p>It can be used to switch between the working and standby sources of synchronization. In other words, the standby source becomes the working source and the working source becomes the standby source.</p> <p>⇒ <b>NOTE:</b> During the switch operation, the <b>Apply</b> and <b>Get</b> buttons are disabled. All fields will be updated as result of this operation.</p>

3. Use the option menus to select appropriate values for **Timing Sync-Mode**, **Primary Source** and **Secondary Source**.
4. Press **Apply** to confirm the changes.
5. Press **Get** to retrieve the active timing references.

6. Press **Switch** to switch between the working and standby sources of synchronization.
7. Click on another tab to change the window or click on **Close** button to exit the window.

#### 5.3.3.4 Set Date and Time

##### Overview

A function required by the AEM-NB is provisioning the date and time of the managed NEs, i.e. the user is able to set the NE Date & Time. Also it is possible for the AEM-NB to retrieve the date and time of any NE.

##### Procedure

Complete the following procedure to set the date and time:

Step	Procedure
1.	Select <b>All -&gt; NE</b> in the Network Browser and <b>NE Information</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> or <b>Equipment -&gt; Provisioning -&gt; Date &amp; Time</b> via the menu bar. The <i>NE Name Information</i> window pops up.
2.	Click on tab <b>Date &amp; Time</b> . (this step is not necessary if the <i>NE Name Information</i> window has been opened via <b>Equipment -&gt; Provisioning -&gt; Date &amp; Time</b> ).

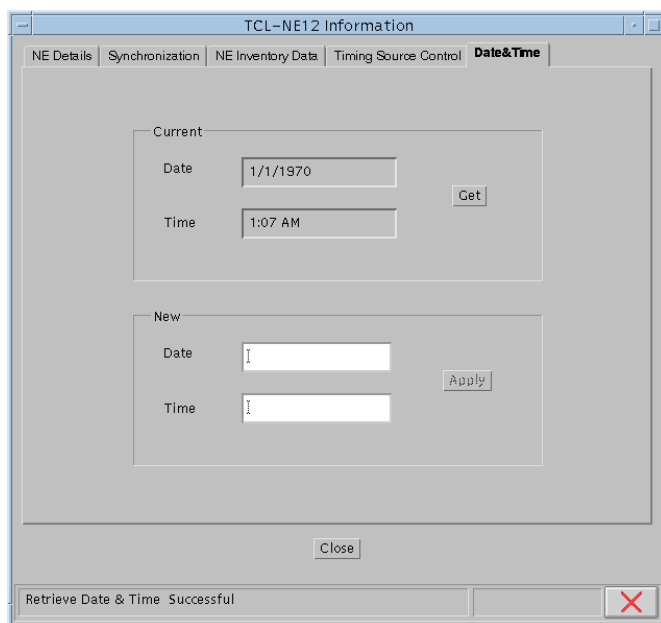


Figure 5-17 "Date & Time" Window

This tab provides you with the facilities needed to obtain the current date and time used in the NE as well as to change them. Two panes are shown: **Current** and **New**.

— **Current**

The current date and time used in the NE is displayed.

Use the **Get** button to retrieve the data from the NE.

— **New**

Enter the **Date** (1980/January/1 to 2036/December/12) and **Time** (12:00 am to 11:59 pm) in order to change the NE date and time.

Press **Apply** to confirm.

This button is active only if a new date and/or new time have been entered.

### 5.3.3.5 Network Element Working Mode

Selection of the working mode via GUI is not yet implemented. It is only possible via Cut-Through interface (cf. Chapter 5.3.7, page 5-74) using T11 commands (Set-CFG-ISDN, SW-CFG).

The system supports an active system configuration which is currently used and a standby system configuration which is set with the command "Set-CFG-ISDN". Possible values for the configurations are: POTS or POTS/ISDN Mixed.

The standby system configuration is activated with the switch configuration command "SW-CFG".

### 5.3.3.6 Configure Simplex COMDAC Protection Scheme

#### Overview

The NE automatically sets the COMDAC protection mode (or duplex mode) when both COMDACs are plugged in. Then the alarming state of both COMDACs slots is set to **Required** and the AEM-NB is not able to change it until one of the COMDACs is removed. When a COMDAC is removed, the AEM-NB is then able to set that slot to **Not-Required**, so the COMDAC protection mode will be disabled (simplex).

#### Procedure

Complete the following procedure to set the COMDAC protection to simplex:

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE -&gt; Shelf -&gt; COM500</b> in the Network Browser and <b>Edit</b> via the cursor menu<br>or select <b>File -&gt; Open</b> or <b>Equipment -&gt; Provisioning -&gt; Edit</b> via the menu bar<br>or single click on the plug-in <b>COMDAC</b> in <i>Shelf View</i> window.<br>The <b>COMDAC</b> window pops up: |
|----|---|

Figure 5-18 "COMDAC" Window



This window includes hardware and software data (inventory) as well as the operational and protection state.

The **Inventory Information** pane contains read-only fields (cf. Chapter 5.3.2.1.3, page 5-32).

For configuring the protection scheme the pane **Operation & Protection** is used.

Parameters/ Buttons	Description
<b>Slot Required</b>	This check box displays the required state of the shelf slot. This state can be changed by the user (from REQUIRED to NOT REQUIRED or vice versa) as long as the plug-in is <b>not</b> inserted. However, it is <b>not</b> possible to set both COMDACs to <b>not</b> required.  The <b>Apply</b> button is available if a change in the <b>Slot Required</b> check box has been made.
<b>Protection State</b>	This non-editable field shows whether the selected COMDAC is working or not: Working (providing service) or Standby (not in service) or Not Equipped (slot is un-equipped).
<b>Protection...</b>	This button provides access to the <i>Shelf Protection</i> window (COMDAC tab) to allow you to modify the current protection scheme or perform protection switching (cf. Chapter 5.3.3.7.1, page 5-60).

2. Deselect the check box **Slot Required**.
3. Click on **Apply** to confirm (the window remains on screen for further use).
4. Click on **Protection...** to open the *Shelf Protection* window (COMDAC tab) (cf. Chapter 5.3.3.7.1, page 5-60) or click on **Close** to exit the window.

### 5.3.3.7 Equipment Protection Switching

#### General

Equipment protection switching provides an automatic recovery mechanism in the *AnyMedia* Access System when a fault is detected. NE entities that are involved in carrying service to a large number of end users are generally required to be protected with a redundant unit. However, the NE provides customer options to have none or some entities protected with redundant units. These entities can be either 1:1 or 1:N protected. For 1:1 protected entities, one of them serves as the active or primary unit and the other serves as a "protection" or standby unit. For 1:N protected entities, one entity serves as the "protection" or standby unit for all N active units. If an active unit fails, the failure is detected and service is automatically "protection switched" to the protection unit. The protection switching can also be requested on demand.

**Revertive/non-revertive**

Equipment protection switching can be revertive or non-revertive. Revertive protection switching implies that the active and standby units will return to their original configuration once the failure causing the protection switch has been repaired. Non-revertive switching does not return the entities to their original configuration. With non-revertive switching, the repaired unit becomes the new standby unit.

The *AnyMedia* Access System R1.3 supports the following protection features:

- COMDAC plug-in - 1:1 protection; non-revertive switch (cf. following section).
- IO\_HDLC packs - 1:1 protection; non-revertive switch - (cf. Chapter 5.3.3.7.2, page 5-63).
- Synchronization reference source - 1:1 protection; non-revertive switch (cf. Chapter 5.3.3.3, page 5-52).

**Definitions**

The different kinds of switching (COMDACs and IO\_HDLC circuit packs) are defined as follows:

- **Side Switching:** refers to the operation of deactivating the active core entity and activating the standby core entity.
- **Manual (normal) Switch:** refers to an AEM-NB-initiated switch command that instructs the NE to perform a switch only if the protection unit is in service and there are no known faults.
- **Forced Switch:** refers to an AEM-NB-initiated switch command that instructs the NE to perform a switch no matter what the conditions of the protection unit.
- **Inhibit Switch:** refers to an AEM-NB-initiated switch command that instructs the NE to inhibit a side switch no matter what the conditions of the active unit.

**5.3.3.7.1 COMDAC Protection Switching****Overview**

The COMDAC is the core plug-in of the *AnyMedia* Access System. The NE supports both duplex and simplex operations, i.e., the COMDAC can be protected or unprotected. In duplex operation, the COMDAC will run in an active and standby mode.

The NE automatically sets the COMDAC protection mode when both COMDACs are plugged in. Then the alarming state of both COMDACs slots is set to **Required** and the AEM-NB is not able to change it until one of the COMDACs is removed. When a COMDAC is removed, the AEM-NB is then able to set that slot to **Not-Required**, so the COMDAC protection mode will be disabled (simplex).

**Procedure**

Complete the following procedure to define protection switching for the COMDAC.

---

Step	Procedure
------	-----------

---

1. Select **All -> NE -> Shelf** in the Network Browser and **Protection** via the cursor menu  
or select **Equipment -> Protection** via the menu bar.  
The *Shelf Protection* window pops up (tab COMDAC).

This window can also be reached from the *COMDAC* window (cf. Chapter 5.3.2.1.3, page 5-32) via **Protection....**

---

The screenshot shows the 'Shelf Protection' window with the 'COMDAC' tab selected. The 'NE Name' field contains 'TCL-NE13'. Below it, the 'COMDAC' tab is active, and the 'IO-HDLC' sub-tab is also visible. The 'Protection Schema' section shows 'Duplex' selected. The 'COMDAC Information' section displays two rows: 'COMDAC1' with status 'Working' and 'SW Version' '01.03.04', and 'COMDAC2' with status 'Standby' and 'SW Version' '01.03.04'. The 'Protection Switch' section has three radio buttons: 'Clear' (selected), 'Forced Switch to Protection', and 'Inhibit'. An 'Apply' button is located to the right of these options. The 'Protection Mode' section shows 'Clear' selected. At the bottom, there is a 'Close' button and a red 'X' icon in the bottom right corner.

**Figure 5-19 "Shelf Protection" Window (Tab COMDAC)**

This window provides COMDAC protection information. It also provides the mechanisms needed to perform changes in the protection scheme as well as protection switches.

The following table shows the view/edit options of the *Shelf Protection* window (tab COMDAC):

Parameters/ Buttons	Description
<b>Protection Schema</b>	Represents the protection scheme used in the NE. If only one COMDAC is present in the shelf, the protection scheme is <b>Simplex</b> . If both COMDACs are present, <b>Duplex</b> is the value shown. Only in this case (Duplex configuration) is the <b>Protection Switch</b> pane available (see below).
<b>COMDAC Information</b>	<b>COMDAC 1 (2):</b> This non-editable fields display the current COMDAC working state. The following values are possible: Working, Standby and Not Equipped (if there is no COMDAC inserted in the corresponding slot).  <b>SW Version:</b> Shows the SW Version for the respective COMDAC.
<b>Protection Switch</b>	Radio buttons allow protection switching to be specified. Only the working COMDAC is inhibited. With the <b>Forced Switch to Protection</b> request the working COMDAC becomes standby and vice versa. All radio buttons are disabled if the current protection scheme is <b>Simplex</b> . The NE rejects a switch request if the <b>Protetion Mode</b> is <b>Inhibit</b> . Therefore before you can switch from <b>Forced Switch to Protection</b> to <b>Inhibit</b> or vice versa you have to <b>Clear</b> the current protection.
<b>Protection Mode</b>	This field displays the current protection mode which will be updated as a result of a protection switch. Possible values: Clear, Inhibit.

2. Use the Radio buttons in field **Protection Switch** to switch the protection: **Clear** or **Forced Switch to Protection** or **Inhibit**.
3. Press **Apply** to confirm. A *Warning* window pops up:

**Protection switching may be service affecting.  
Do you want to continue?**

If you decide to continue, the switch operation will be started. The information displayed will be updated once the switch is finished to show the current state.

The following events set off error messages:

- The NE detects an error in the switch request (i.e. the request cannot be executed due to another activity in the AEM-NB).
- The NE rejects a switch request because the **Protetion Mode** is **Inhibit**.
- The NE cannot execute the request as the NE software installation is in progress.

- Click on tab HDLC to change the window (see next section) or click on **Close** to exit the window.

### 5.3.3.7.2 IO\_HDLC Protection Switching

#### Overview

For the IO\_HDLC plug-in 1:1 protection applies where one IO\_HDLC plug-in serves as the active or primary and the other serves as a "protection" or standby unit. If an active unit fails, the failure is detected and service is automatically "protection switched" to the protection unit. The protection switching can also be requested on demand. IO\_HDLC protection switching is only possible in R1.3.

#### Procedure

Complete the following procedure to define protection switching for IO\_HDLC.

Step	Procedure
------	-----------

- Select **All -> NE -> Shelf** in the Network Browser and **Protection** via the cursor menu  
or select **Equipment -> Protection** via the menu bar.  
The **Shelf Protection** window pops up:
- Click on tab **IO\_HDLC**.

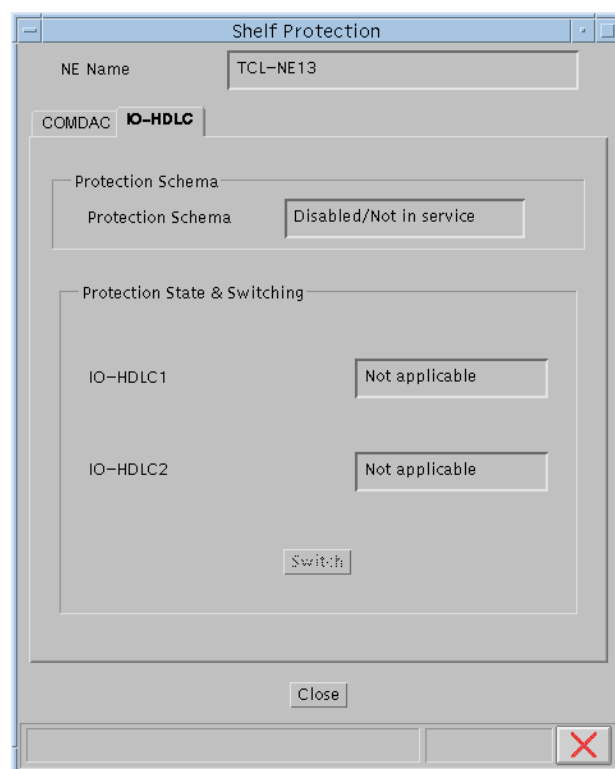


Figure 5-20 "Shelf Protection" Window (Tab IO\_HDLC)

This window provides IO\_HDLC protection information. It also provides the mechanisms needed to perform changes in the protection scheme as well as protection switches.

The following table shows the view/edit options of the *Shelf Protection* window (tab IO\_HDLC):

Parameters/ Buttons	Description
<b>Protection Schema</b>	<p>This field shows the protection schema for IO-HDLCs used in the NE.</p> <p>Possible values:            Enabled (if switching between IO_HDLCs is enabled)            Disabled / Not Equipped,            Disabled / Not in service (i.e. the card is not pre-provisioned or its administrative state is locked) or            Disabled / POTS only mode (if switching between IO_HDLCs is not enabled).</p>
<b>Protection State and Switching</b>	<p><b>IO-HDLC 1 (2):</b> This non-editable fields display the current IO-HDLC working state.</p> <p>Possible values: Working, Standby and Not applicable (if there is either no IO_HDLC inserted in the corresponding slot, no IO_HDLC provisioned for this slot or the NE is operating in POTS only mode, or a combination of the previous conditions).</p> <p>The <b>Switch</b> button is enabled if the protection schema is enabled.</p> <p>In that case, pressing the button causes the working/standby states to be switched in the NE.</p>

- Press **Switch** to switch the protection state. The *Warning* window pops up:

**Protection switching may be service affecting. Do you want to continue?**

If you decide to continue, the switch operation will be started. The information displayed will be updated once the switch is finished to show the current state.

The following events set off error messages:

- The NE detects an error in the switch request (i.e. the request cannot be executed due to another activity in the AEM-NB).
- The NE cannot execute the request as the NE software installation is in progress.
- The forced switch is denied as the protecting slot is locked out.

- The manual switch is denied either because there is a higher protection switch active (Inhibit, Forced) or because an automatic switch is already protecting that protected slot.
4. Click on **Close** to exit the window.

### 5.3.3.8 Alarm Configuration

Configuring of the alarm severities is only possible via the cut-through interface (cf. Chapter 5.3.7, page 5-74). The corresponding TL1 commands are available on-line using the GSI help on *AnyMedia* Access System.

## 5.3.4 Network Element Software Upgrade

This function is subdivided into two parts: NE software download and program copy.

### 5.3.4.1 Network Element Software Download

#### Overview

There are two software versions, the one in the active COMDAC and the new one to be downloaded (must be placed in \$ANYMEDIA/CM/nefiles/NVPS). It is assumed that the user has a copy of the software currently running in the active COMDAC.

The software download procedure is as follows:

- start download
- load software into the standby COMDAC.

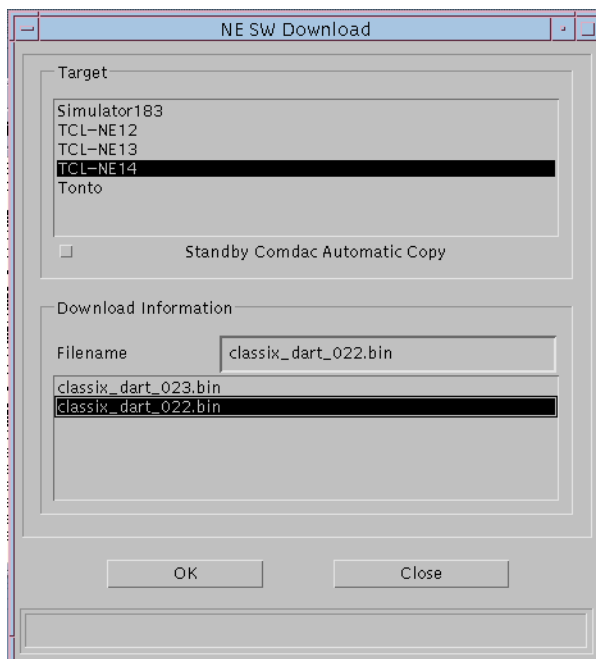
#### Assumptions

For the following description it is assumed that the NE is already connected and the NE hardware platform is prepared to receive and work with the new program version.

#### Procedure

Complete the following procedure to start software download:

Step	Procedure
1.	Select <b>All</b> or <b>All -&gt; NE</b> in the Network Browser.
2.	Select <b>Equipment -&gt; NE SW Download</b> via the menu bar. The <i>NE SW Download</i> window pops up:



**Figure 5-21 "NE SW Download" Window**

This window is subdivided into two fields: **Target** and **Download Information**.

If coming from All level (**All**) the **Target** pull-down list displays all NEs. It Allows to select the set of NEs on which the software download is to be made by clicking on NEs in the pull-down list. The selected NEs in the list will be highlighted.

If coming from NE level (**All -> NE**) this field is a non-editable text field already filled with the name of the NE selected at the NE level.

3. Select one or more NEs in the Target list (if coming from All).
4. Set the check box **Standby Comdac Automatic Copy** if you want to copy automatically the software from the working comdac to the standby COMDAC after the software download is completed successfully.
5. Select a desired file in the **Download Information** list. The corresponding file will be displayed in the **Filename** field.
6. Click on **OK**. A *Warning* window pops up (the *Software Download* window remains on the screen after the download is finished):

**SW Download is service affecting. Do you want to continue?**



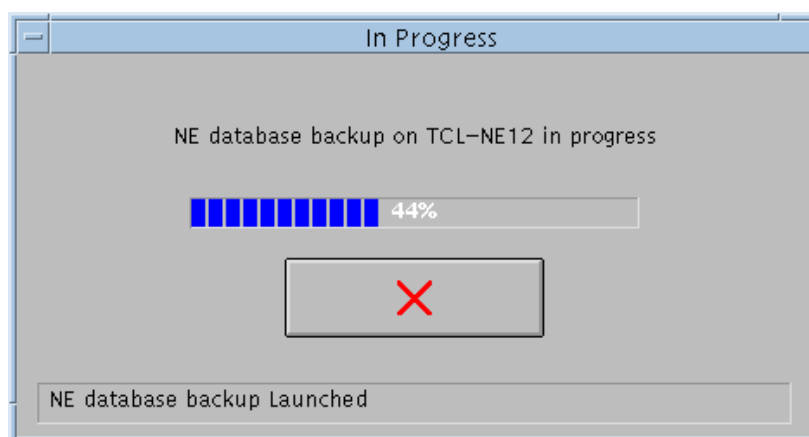
If you decide to continue the AEM-NB starts the download procedure. An *In Progress* window pops up showing the following message:

SW Download to <NE Name> in progress.



**NOTE:**

The *In Progress* window is a dialogue window with progress indicator and cancel option that will be displayed any time there is a long duration task being performed, such as SW Download. The following figure shows an example:



**Figure 5-22 Example of an "In Progress" Window**

A download progress indicator will be shown in the progress bar. The software download operation consists of an FTP operation and an initialization of the NE after the FTP operation. The status bar shows which of these two operations is currently active. The progress bar shows how much of the FTP transfer is complete. After the FTP transfer has finished a new progress window pops up. In this window the progress bar will reach the 90% mark after 5 minutes (this time can be configured in a preferences file). Then the progress bar continually shows 90% until the connection between the AEM-NB and the NE is established again. The **Cancel** button will be disabled if the SW Download command is executed (i.e. an FTP process is still running).



**NOTE:**

The SW download process cannot be cancelled.

7. Wait until this process is finished.

The following errors will stop the download process:

- NE does not match login and password. The AEM-NB returns operation failed to the AEM-NB.
- NE detects that the side switch to the standby COMDAC is not possible (e.g. 2nd COMDAC not present) and refuses the SW Download operation.
- If the download of the data fails an alarm is issued and manual intervention will be required to:
  - restart the download procedure from the beginning, or
  - write from the active COMDAC to the standby COMDAC to back out the partial load (duplex configuration) - see Chapter 5.3.4.2, page 5-69.
- If the software program is not installed successfully on the standby COMDAC:

In duplex configuration, an alarm will be sent to the AEM-NB and manual intervention will be required to:

  - restart the download procedure from the beginning, or
  - write from the active COMDAC to the standby COMDAC to remove the downloaded copy - see Chapter 5.3.4.2, page 5-69.
- The TCP connection between AEM-NB and NE is lost.

### 5.3.4.2 Program Copy

#### Overview

This function is used to copy a new loaded software from the currently active COMDAC to the standby COMDAC. During normal operation both COMDACs should have the same software version. So the software copy should always be the next step after software download except software copy is started automatically after software download (cf. previous chapter).

#### Duplex Configuration

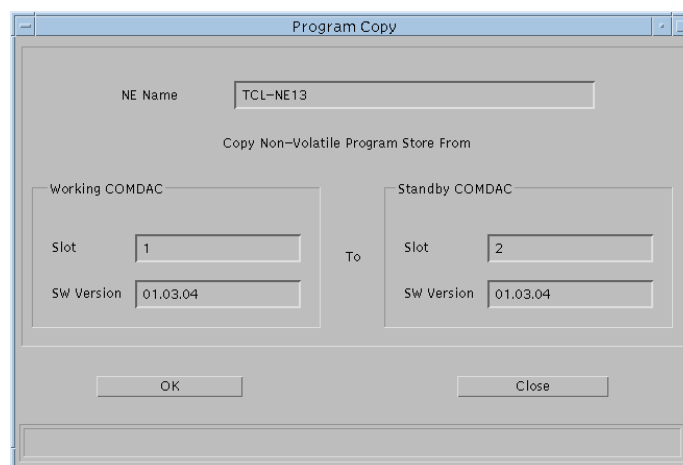
For the following description it is assumed that the NE is configured in duplex configuration.

#### Procedure

Complete the following procedure to copy the new software from the active COMDAC to the standby COMDAC:

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE -&gt; Shelf</b> in the Network Browser and <b>Program Copy</b> via cursor menu or select <b>Equipment -&gt; Program Copy</b> via the menu bar. The <i>Program Copy</i> window pops up: |
|----|---|



**Figure 5-23 "Program Copy" Window**

This is a dialogue window requesting information from the user to continue. There are two panes (titled **Working COMDAC** and **Standby COMDAC**) showing the corresponding slot number and SW versions used in each of the COMDACs.

#### — Slot

Identifies which COMDAC is where (e.g. Working COMDAC in slot 1 and Standby in slot 2).

— **SW Version**

Obtained from the NE. The SW version of the working COMDAC will be taken as the NE SW version.

2. Press **OK** to start the software copy. An *In Progress* window pops up:

**Program Copy from COMDAC 1 to COMDAC 2 in Progress**

3. Wait until this process is finished.

### 5.3.5 Nonvolatile Data Storage (NVDS)

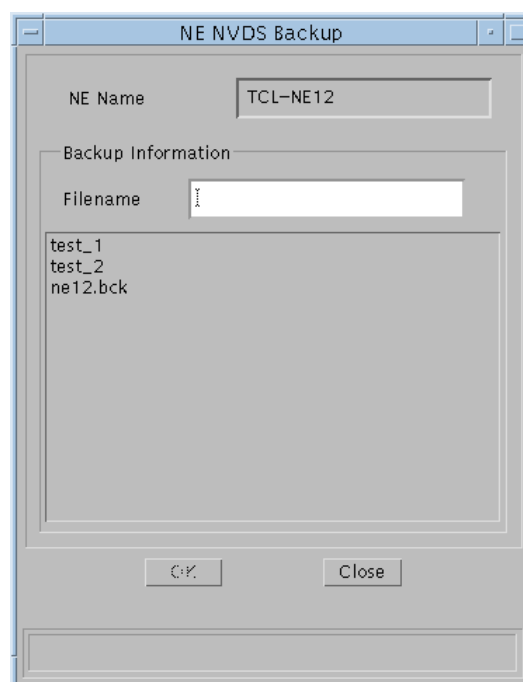
<b>Overview</b>	This section describes the backup and restore procedures. The backup procedure uploads the data from the NE's COMDAC to the AEM-NB. The restore function deals with the downloading of a previous backup NVDS from the AEM-NB to the NE. Both functions apply to both simplex and duplex NE configurations.
<b>Backup/Restore Data</b>	For database backup and restoration the AEM-NB is able to create/maintain a copy of provisioning data from the active COMDAC (NVDS). When a loss of data occurs in the NE (due to factors such as human error, power failure or hardware and software failures), the restoration features enable the AEM-NB to restore a previous backup to one NE.
<b>Backup Media</b>	The AEM-NB is able to store the backup copy in diverse storage media that can include Hard Disk Drive (HDD), tapes, removable disk cartridges and any other available mass-storage medium.
<b>FTP</b>	<p>For database backup and restoration operations the AEM-NB uses a File Transfer Protocol (FTP) connection within the NE. FTP allows the AEM-NB to overwrite or copy information residing on the NE.</p> <p>The AEM-NB can open only one FTP session per NE at a time where the AEM-NB will support the client role of the FTP session, and the <i>AnyMedia</i> Access System will play the server part.</p>
<b>Failing Backup/Restore</b>	The backup and restore processes will fail if the time period during which the connection is lost exceeds the time-out defined in the AEM-NB or the NE time-out; otherwise the process will continue after the connection is recovered.

### 5.3.5.1 Data Backup

**Procedure** Complete the following procedure to initiate data backup:

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE</b> in the Network Browser   |
| 2. | Select <b>Equipment -&gt; NE NVDS Backup</b> via menu bar. The <i>NVDS Backup</i> window pops up: |



**Figure 5-24 "NVDS Backup" Window**

The **Filename** list displays all file names available for a backup.

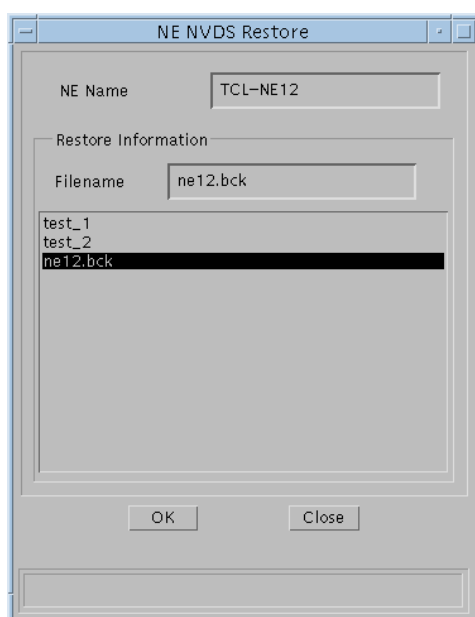
3. Select the file in the list of which you wish to make a backup. The corresponding file will be displayed in the **Filename** field and can be edited.
4. Click on **OK** (this command button is available only after having selected the file name). The status bar shows the progress of the operation. Depending on the configuration the backup process can take up to seven minutes.

### 5.3.5.2 Data Restore

**Procedure** Complete the following procedure to initiate data Restoration:

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE</b> in the Network Browser   |
| 2. | Select <b>Equipment -&gt; NE NVDS Restore</b> via menu bar. The <i>NVDS Restore</i> window pops up: |



**Figure 5-25 "NVDS Restore" Window**

The **Filename** list displays all backup file names.

3. Select a desired file in the list. The corresponding file will be displayed in the **Filename** field and can be edited.
4. Click on **OK** (this command button is available only after having selected the file name). A *Warning* window pops up:

**NE NVDS Restore may be service affecting. Do you want to continue?**

5. Press **Yes** to confirm this message. An *In Progress* window pops up:

**NVDS restore on <NE Name> in progress**

6. Wait until this process is finished.

**NOTE:**

When a NVDS restore process is started, all AEM-NB variables are set to their initial values to provoke a FULL synchronization. The NE synchronization state goes to ASYNC.

The association between AEM-NB and NE is lost and recovered. The FULL synchronization is launched for that NE.

Finally, the NE is connected and perfectly synchronized.

### 5.3.6 Network Element Reset

This menu is used to reset the NE's NVDS to the factory default except for the IP address and the target identifier, so that the AEM-NB can still communicate with the NE after command execution is complete.

**Procedure**

Complete the following procedure to get the inventory data:

Step	Procedure
1.	Select <b>All -&gt; NE</b> in the Network Browser.
2.	<p>Select <b>Equipment -&gt; NE Reset (INIT-SYS)</b> via the menu bar. A <i>Warning</i> window pops up:</p> <p><b>NE Reset is service affecting. The data stored in the NE Name will be destroyed and set to the default manufacturing values. Do you want to continue?</b></p> <p>If you decide to continue, the AEM-NB will send an INIT-SYS to the NE to reset the NVDS to its default values and launch the following message in the <i>In Progress</i> window.</p> <p><b>Reset &lt;NE Name&gt; in progress</b></p>

**NOTE:**

A progress indicator for the reset is shown in the *In Progress* window. This indicator will reach the 90% mark 5 minutes (this time can be configured in a preferences file) after the NE Reset operation was started and will then show this value until the connection between the AEM-NB and the NE is established again.

**NOTE:**

After the reset process has finished correctly the connection to the NE is automatically re-established.

### 5.3.7 TL1 Cut-Through

#### Overview

The AEM-NB provides the user with a command line to a TL1 (transaction language 1) session with any NE. Using this command line, the user can type any TL1 command, send these commands to a selected NE and get the responses to the requests as well as all the autonomous outputs sent by the NE.

TL1 used for the provisioning, maintenance and administration of the *AnyMedia* Access System is an ASCII-based command language.

This cut-through interface is used by remote AEM-NB craft personal when the GUI does not support certain TL1 commands. The AEM-NB will provide the independence between the cut-through interface and the GUI interface.

To open a cut-through interface with an NE the operator must provide the connection information (Login and Password) defined in the NE Name Information window (cf. Chapter 5.3.1, page 5-17).

When the AEM-NB receives the request to open a cut-through session, it opens a telnet connection with the selected NE, to avoid conflicts with the current AEM-NB GUI session. Then the operator will manage the cut-through session through the use of TL1 commands.

#### Cut-through / GUI independence

The AEM-NB GUI behaviour (but not necessarily the performance) is not affected by any simultaneous cut-through connection running on the platform.

The operator using the AEM-NB GUI need not have to know about any cut-through session running on the AEM-NB platform. The performance of the system could be affected by the load of the hardware, but the behaviour of the GUI is the same in both cases.

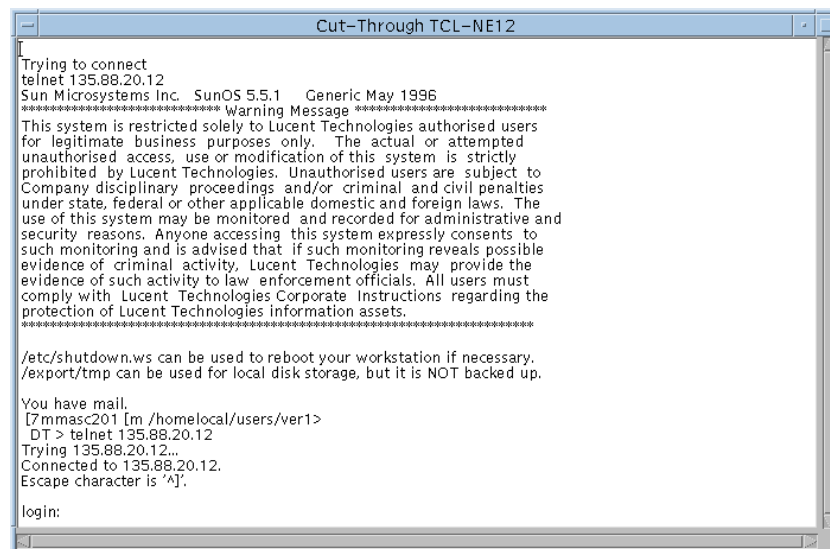
#### Procedure

Complete the following procedure to start a TL1 session:

1. Select **All -> NE** in Network Browser.
2. Select **TL1 -> Cut-through** via the menu bar to start a TL1 session. The *Cut through* window pops up.

#### How to start a TL1 session





**Figure 5-26 "Cut Through" Window**

3. Enter the **Login** and **Password** as defined in the *NE Name Information* window (cf. Chapter 5.3.1, page 5-17).

Now you are able to enter the appropriate TL1 commands.

The TL1 descriptions (syntax, formats, parameters, ...) are available on-line using the GSI help on *AnyMedia* Access System.

### 5.3.8 Delete Network Element

If the NE should not be managed by the AEM-NB any longer, it shall be deleted from the AEM-NB database.

#### Procedure

Complete the following procedure to delete an NE.

Step	Procedure
------	-----------

1. Select the **All -> NE** in the Network Browser and **Delete** via the cursor menu or select **File -> Delete** or **Equipment -> Provisioning -> Delete** via the menu bar. A *Warning* window pops up:

**You are about to delete <NE Name>. Do you want to continue?**

If you select **No**, the deletion of the NE is rejected. Otherwise, the NE will be deleted.

**NOTE:**

When an NE is deleted from the AEM-NB database, it is still fully functional. The TL1 and TCP/IP links between the AEM-NB and the NE will be closed and the management access via the AEM-NB is finished until the NE is created and connected again.

## 5.4 Service Provisioning

### Provisioning Summary

Prior to service activation on the AEM-NB several data items need to be provisioned. It is necessary to configure cross-connections between ports and logical and physical entities and vice versa. In addition it is necessary to specify the service type (V5.1, V5.2, POTS, ISDN or permanent leased lines (PLL)).

### Supported Interfaces

Figure 5-27, page 5-78 is a functional diagram of the cross-connections between the physical (E1 and subscriber) ports of the system and the logical entities. The AEM-NB supports

- up to 16 V5.1
- up to 16 V5.2
- up to 16 PLL interfaces

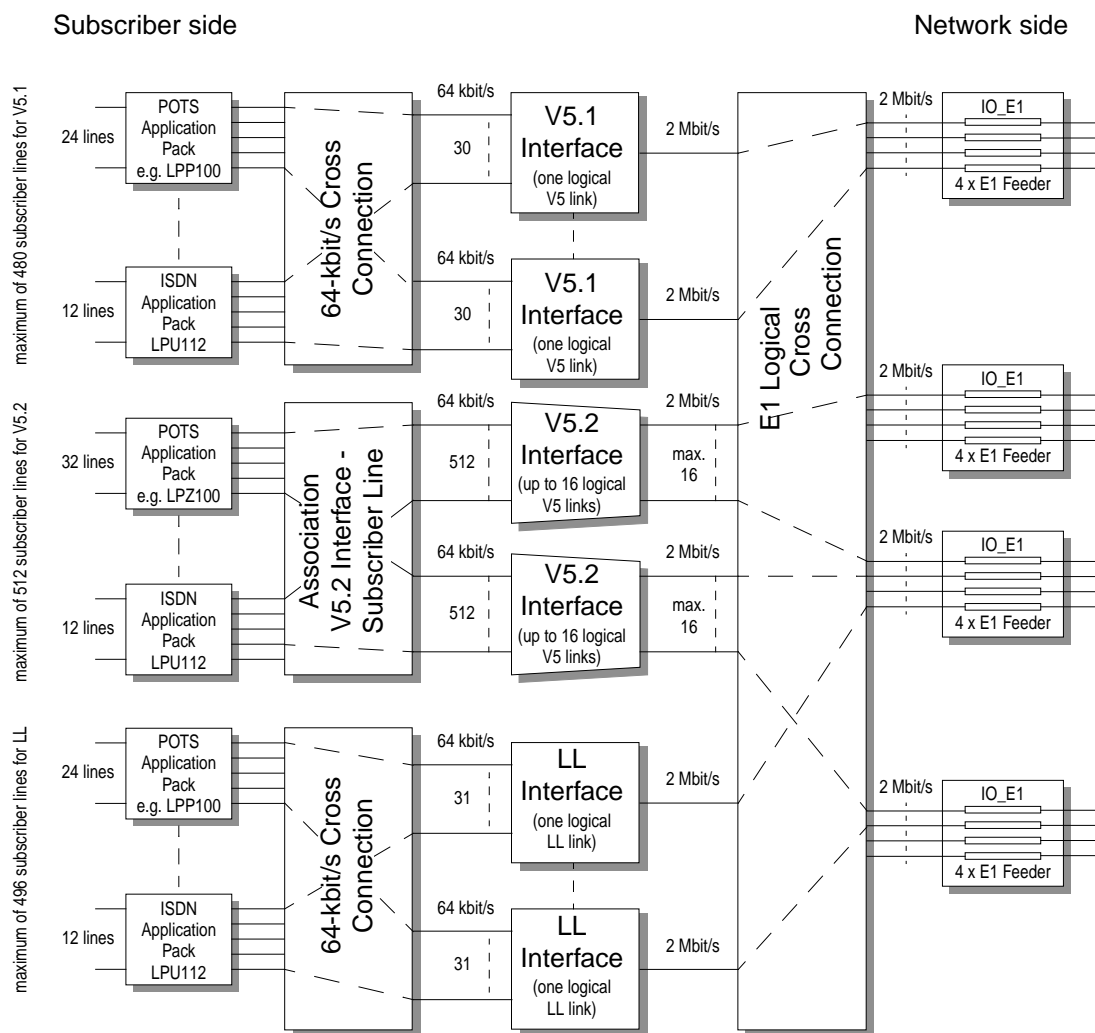
in any combination not exceeding the maximum of 16 E1 feeders in the system.

### 2 Mbit/s Cross-Connections

E1 logical cross-connections provide 2-Mbit/s bandwidth to the interfaces. A maximum of 16 E1 cross-connections can be created; they are limited by the maximum number of E1 feeder ports in the system.

### 64 kbit/s Cross-Connections

64-kbit/s cross-connections bind a Z port to a V5.1 or PLL timeslot to a V5.2 Interface. A maximum of 513 64-kbit/s cross-connections can be created; they are limited by the maximum number of Z ports in the system (512), plus the one remote operations channel (ROC).



**Figure 5-27 Functional Diagram of Cross-Connects Within the AEM-NB**

#### Ports/Lines

Each interface contains the provisioning data for its E1 ports. 64-kbit/s and E1 cross-connections provide the linkage between the used protocol and the corresponding physical interfaces.

Each V5.1 Interface supports one E1 port (2 Mbit/s) and 30 subscriber lines (64 kbit/s).

Each V5.2 Interface supports up to 16 E1 ports (2 Mbit/s) and up to 512 subscriber lines (64 kbit/s).

Each leased line interface supports one E1 port (2 Mbit/s) and up to 31 analog or digital leased lines (64 kbit/s).

**NOTE:**

A mix of services (V5.x and leased lines) on one E1 feeder is not possible.

**V5 Protocol**

V5 protocol is an ETSI (European Telecommunication Standards Institute) defined interface protocol between a Local Exchange (LE) and an NE for the support of the following access types:

- Analogue telephone access: POTS (Plain Old Telephone Service)
- ISDN Basic Rate Access: ISDN-BRA
- Other analogue or digital accesses for permanent connections

with provisionable information channel allocation or flexible concentration capability within the NE.

**NOTE:**

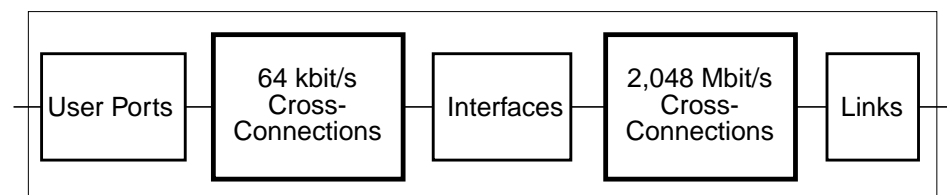
ISDN Primary Rate Access will be possible in future releases.

**Supported Subscribers**

The general V5 protocol purpose is to connect PSTN (Public Switched Telephone Network) and ISDN subscribers (via V5 Interface) and leased subscribers to the LE. ETSI distinguishes between V5.1 Interfaces which only allow to connect PSTN and ISDN-BRA subscribers and V5.2 Interfaces which allow to connect ISDN PRA subscribers as well.

**Cross-Connections**

A single NE can contain a number of V5 User Ports, a number of V5 Interfaces and a number of V5 Links (which represent 2,048 Mbit/s links). There is a bi-directional association (cross-connection) between each V5 Interface and all of its related V5 User Ports. Likewise there is a bi-directional relationship between each V5 Interface and all its related V5 Links.



**Figure 5-28 Cross-Connections**

From the management point of view, a V5 Interface can be represented by a set of logical manageable entities with their own configuration data and relations (cross-connections) that are established by provisioning.

**Interfaces - Links**

The NE may contains up to 16 V5 Interfaces and up to 16 V5 Links (16 E1 physical feeders limitation). On the other hand, for *AnyMedia* Access System a limitation of 512 subscribers (V5 User Ports) arises from the 32-channel POTS APs.

**Communication Channels, Paths and Timeslots**

Only one V5 Link can be associated to a V5.1 Interface and up to 16 V5 Links can be associated to a V5.2 Interface. For both V5.1 and V5.2 Interfaces, the association of user signalling with communication paths (CP) and the association between CPs and logical communication channels (CC) have to be provisioned. The association of CCs with physical communication timeslots (TS) is initially provisioned (configured) but can be changed within V5.2 Interfaces by the V5.2 protection protocol.

For more information refer to the NE documentation for R1.3.

**Screen Navigation**

Figure 5-29, page 5-81 shows an overview of the screen navigation for service provisioning.

The arrows represent the order in which the windows can be opened.

**Example**

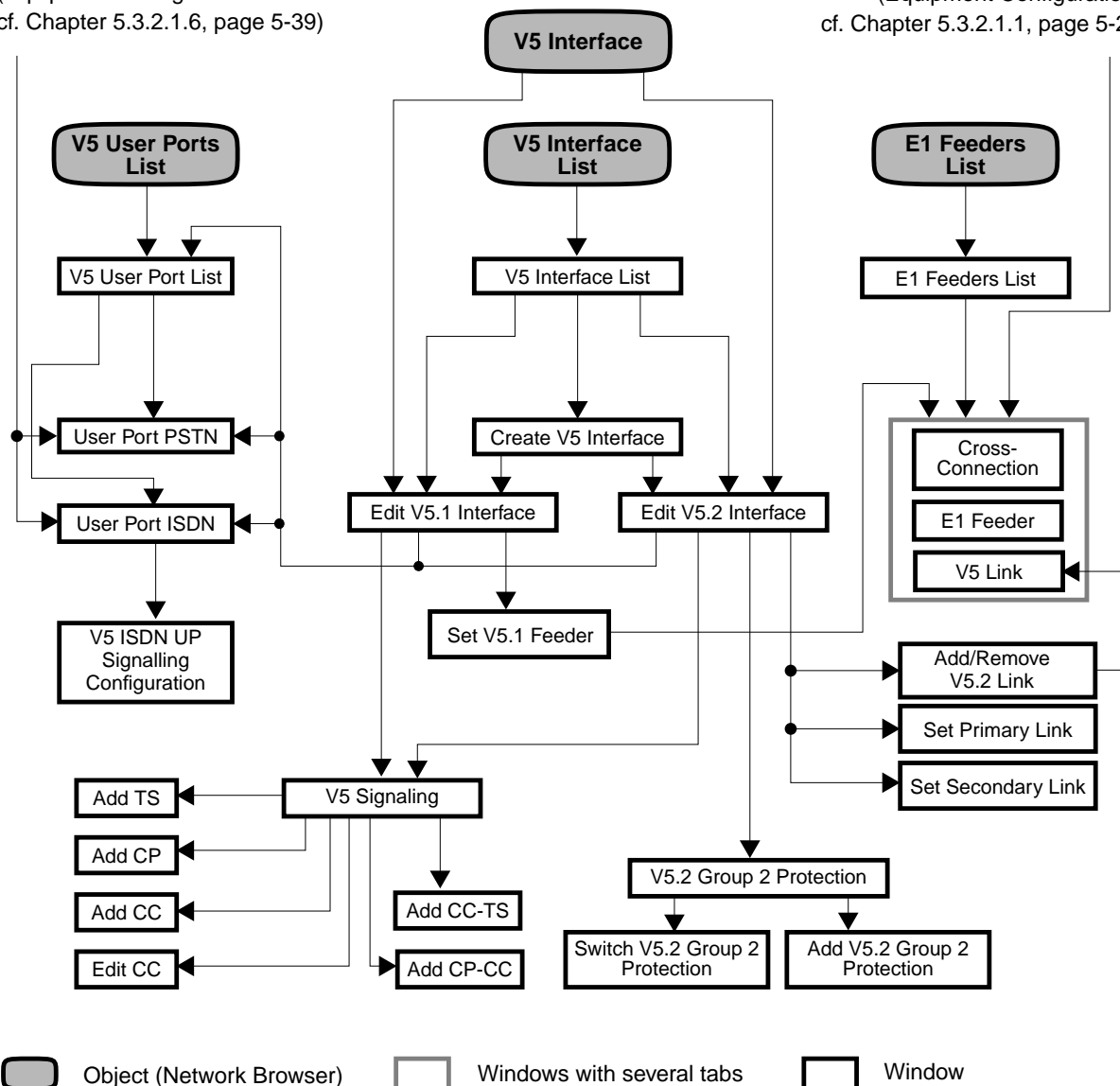
To edit the *V5.1 Interface* window

- select **All -> NE -> V5 Interfaces List -> V5 Interface id** in the Network Browser and  
select **Edit** via the cursor menu.

from AP window

(Equipment Configuration -  
cf. Chapter 5.3.2.1.6, page 5-39)

from IO\_E1 window

(Equipment Configuration -  
cf. Chapter 5.3.2.1.1, page 5-26)**Figure 5-29 Screen Navigation for Service Provisioning**

The next sections describe the most common way for provisioning a V5 Interface and the related services:

- Create V5 Interface.
- Add V5 Links.
- Define primary V5 Links (V5.2 Interfaces only).
- Define secondary V5 Links (V5.2 Interfaces only).

- Create communication channels.
- Define communications channels for PSTN protocol.
- Define communications channels for ISDN signalling protocol.
- Create communications channels to be protected and timeslots to protect them.
- Create ISDN communication paths (subscriber groups).



### 5.4.1 Create a V5 Network Interface

#### Overview

The maximum number of V5 Interfaces that can be supported by the *AnyMedia* Access System is 16, so the AEM-NB can prevent the user at GUI level that a V5 Interface creation operation will be rejected if this number is exceeded or if provisioning information is not correct (V5.2 Interface identifier must be unique within the managed access network).

#### Procedure

Complete the following procedure to create a V5 Interface.

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE -&gt; V5 Interface List</b> in the Network Browser and <b>Edit</b> via the cursor menu<br>or select <b>File -&gt; Open</b> or <b>Service -&gt; Provisioning -&gt; Edit</b> or <b>Service -&gt; V5 Interface List</b> via the menu bar. The <i>V5 Interfaces List</i> window pops up. |
|----|---|

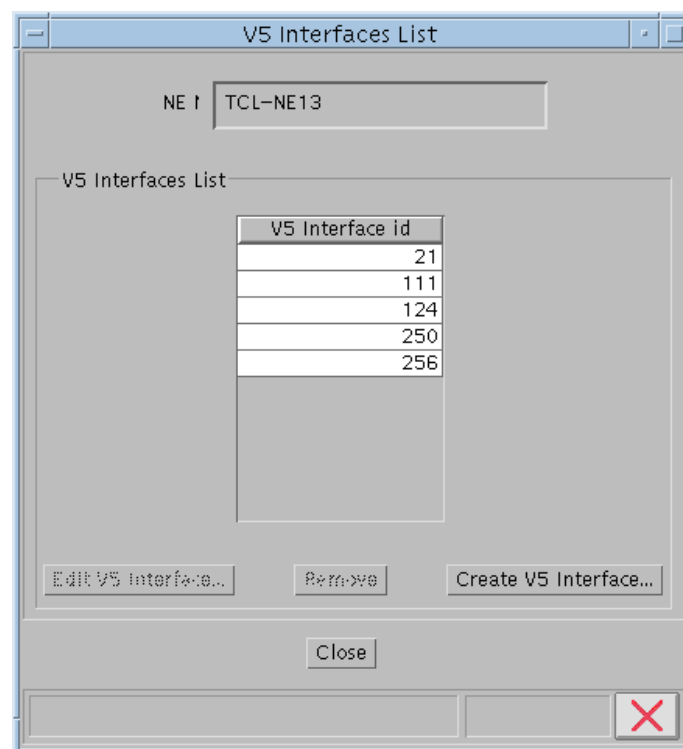


Figure 5-30 "V5 Interface List" Window

Parameters/ Buttons	Description
<b>V5 Interface Id</b>	The list displays all available V5 Interface ids.  Upon selection of any entry, the <b>Edit V5 Interface...</b> button becomes available.
<b>Edit V5 Interface...</b>	This button provides access to the <i>V5 Interface</i> window (V5.1 or V5.2; version dependent on protocol version) to edit the data of an already defined V5 Interface.
<b>Remove</b>	This button can be used to remove the selected V5 Interface(s). Removing is only possible if the selected V5 Interface has no V5 Links and V5 User Ports linked, and no contained communication channels nor communication paths.
<b>Create V5 Interface...</b>	This button provides access to the <i>V5 Interface Create</i> window.

If you want to ...	then ...
edit a V5 Interface	select an appropriate entry in the list and click on <b>Edit V5 Interface...</b> or double click on the entry. The <i>V5.x Interface</i> window pops up (cf. Chapter 5.4.1.1, page 5-87 for V5.1, cf. Chapter 5.4.1.2, page 5-90 for V5.2).
remove a V5 Interface	select an appropriate entry in the list and click on <b>Remove</b> . (cf. Chapter 5.4.17, page 5-159).
create a V5 Interface	click on <b>Create V5 Interface....</b> The <i>V5 Interface Create</i> window pops up (see below).

**Figure 5-31 "V5 Interface Create" Window**

This window can also be reached from the menu bar via **Service -> Provisioning -> Create V5 Interface**.

The following table shows the view/edit options of the *V5 Interface Create* window:

Parameters/ Buttons	Description
<b>V5 Interface id</b>	This text field is used to enter the interface id. Possible values: {0, 16777215} or None. Default: None.
<b>Protocol Version</b>	This option menu is used to select the protocol version for this V5 Interface. Possible values: V5.1 and V5.2. Default: V5.2.
<b>Provisioning Variant</b>	This text field is used to enter a short integer for the provisioning variant. Possible values: {0, 127}. Default: 0.
<b>Service Degrading Threshold</b>	This text field is used to enter a short integer for the service degrade threshold. Possible values: {5, 95}, step 5. Default: 50.
<b>HDLC Flag Monitoring</b>	This option menu can be used to define the HDLC Flag Monitoring condition. Possible values: Yes or No. Default: Yes.

Parameters/ Buttons	Description
<b>Create</b>	This button is used to confirm the creation of the V5 Interface with the given parameters. It is available only if the user has specified a value for the V5 Interface id.

2. Enter an appropriate **V5 Interface id**.
3. Use the option menu **Protocol Version** to select the appropriate version.
4. Enter the desired values for **Provisioning Variant** and **Service Degrade Threshold**.
5. Use the option menu **HDLC Flag Monitoring** to define the monitoring condition.
6. Click on **Create** to confirm the entries. The *V5.x Interface* window pops up (only possible if the maximum of 16 V5 Interfaces is not yet exceeded and in case of V5.2 protocol the **V5 Interface id** is unique within the whole managed network).
7. Go to Chapter 5.4.1.1, page 5-87 for editing V5.1 Interface or go to Chapter 5.4.1.2, page 5-90 for editing V5.2 Interface.

**NOTE:**

When a V5.1 Interface is created and configured the communication path *Control* is automatically created

When a V5.2 Interface is created and configured the communication paths *Control*, *Link* and *BBC* are automatically created (cf. Add Communication Path - Chapter 5.4.6.4, page 5-140).

### 5.4.1.1 Edit V5.1 Interface

Each V5.1 Interface supports one E1 port (2 Mbit/s) and up to 30 subscriber lines (64 kbit/s).

#### Procedure

Complete the following procedure to edit a V5.1 Interface.

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>Service -&gt; V5 Interface List</b> via the menu bar, select the desired <b>V5 Interface id</b> in the <i>V5 Interface List</i> window and click on <b>Edit V5 Interface....</b> The <i>V5.1 Interface</i> window pops up. |
|----|---|

This window can also be reached from the *V5 Interface Create* window by clicking on **Create** (cf. Figure 5-31, page 5-85).

**Figure 5-32 "V5.1 Interface" Window**



#### NOTE:

The parameters in this window can only be modified if the administrative state is "Locked".

The following table shows the view/edit options of the *V5.1 Interface* window:

Parameters/ Buttons	Description
<b>V5.1 Interface Data</b>	<p><b>V5 Interface Id</b>, <b>Provisioning Variant</b> and <b>Service De-grade Threshold</b> shows the values as described in Chapter 5.4.1, page 5-83.</p> <p>The option menu <b>HDLC Flag Monitoring</b> can be used to define the HDLC Flag Monitoring condition.</p> <p>Possible values: Yes or No.</p> <p>The option menu <b>Administrative State</b> can be used to select the administrative state for the V5.1 Interface.</p> <p>Possible values: Locked, Unlocked.</p> <p>After creation the interface is always "Locked".</p> <p><b>Operational State</b>: Shows the current operational state of this V5 Interface.</p> <p><b>Get</b>: This button can be used to get the current operational state from the NE.</p> <p>The <b>Apply</b> button is used to confirm the changes in the V5.1 Interface Data field.</p>
<b>Command buttons</b>	<p>The <b>V5 User Ports...</b> button provides access to the <i>V5 User Port List</i> window, limited to the user ports that are linked to this V5 Interface.</p> <p>The <b>Add PSTN...</b> button provides access to the <i>V5 PSTN User Port</i> window, where the V5.1 Interface is displayed (and cannot be modified).</p> <p>The <b>Add ISDN...</b> button provides access to the <i>V5 ISDN-BRA User Port</i> window, where the V5.1 Interface is displayed (and cannot be modified).</p> <p>The <b>Signalling...</b> button provides access to the <i>V5 Signalling</i> window for this V5.1 Interface.</p>
<b>Link</b>	<p>The <b>Physical Feeder</b> field shows the id that is linked to this V5.1 Interface, if there is one.</p> <p>The <b>Set Feeder...</b> button provides access to the <i>V5.1 Set Feeder</i> window. This button is enabled only when the <b>Administrative State</b> is "Locked"</p> <p>The <b>Remove</b> button can be used to delete the selected feeder. This button is only available if there is a feeder already set and the V5 Interface state is "Locked".</p>

<b>If you want to ...</b>	<b>then ...</b>
edit the V5 Interface parameters	change the parameters in the field <b>V5 Interface</b> and click on <b>Apply</b> to confirm. If the administrative state has been changed from "Unlocked" to "Locked" a Warning window pops up:  <b>Changing the administrative state of V5 Interface id may be service affecting. Do you want to continue?</b>
edit a V5.1 User Port	click on <b>V5 User Ports....</b> The <i>V5 User Port List</i> window pops up (cf. Figure 5-41, page 5-115).
add a V5.1 User Port PSTN	click on <b>Add PSTN....</b> The <i>V5 PSTN User Port</i> window pops up (cf. Chapter 5.4.5.1, page 5-118).
add a V5.1 User Port ISDN-BRA	click on <b>Add ISDN....</b> The <i>V5 ISDN-BRA User Port</i> window pops up (cf. Chapter 5.4.5.2, page 5-124).
modify the Signalling parameters	click on <b>Signalling....</b> The <i>V5 Signalling</i> window pops up (cf. Chapter 5.4.6).
set a feeder	click on <b>Set Feeder....</b> The <i>V5.1 Set Feeder</i> window pops up (cf. Chapter 5.4.2.1, page 5-94).
remove the physical feeder	click on <b>Remove</b> .
exit the window	click on <b>Close</b> .

### 5.4.1.2 Edit V5.2 Interface

Each V5.2 Interface supports up to 16 E1 ports (2 Mbit/s) and up to 512 subscriber lines (64 kbit/s).

#### Procedure

Complete the following procedure to edit a V5.1 Interface.

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>Service -&gt; V5 Interface List</b> via the menu bar, select the desired <b>V5 Interface id</b> in the <i>V5 Interface List</i> window and click on <b>Edit V5 Interface....</b> The <i>V5.2 Interface</i> window pops up. |
|----|---|

This window can also be reached from the *V5 Interface Create* window by clicking on **Create** (cf. Chapter 5.4.1, page 5-83).

**Figure 5-33 "V5.2 Interface" Window**



**NOTE:**

The parameters in this window can only be modified if the administrative state is "Locked".

The following table shows the view/edit options of the *V5.2 Interface* window:

Parameters/ Buttons	Description
<b>V5.2 Interface Data</b>	<p><b>V5 Interface Id, Provisioning Variant</b> and <b>Service Degradation Threshold</b> shows the values as described in Chapter 5.4.1, page 5-83.</p> <p>The option menu <b>HDLC Flag Monitoring</b> can be used to define the HDLC Flag Monitoring condition.</p> <p>Possible values: Yes or No.</p> <p>The option menu <b>Administrative State</b> can be used to select the administrative state for the V5.2 Interface.</p> <p>Possible values: Locked, Unlocked.</p> <p>After creation the interface is always "Locked".</p> <p>Changing this and confirming is only successful if the rest of the configuration is complete.</p> <p><b>Operational State:</b> Shows the current operational state of this V5 Interface.</p> <p><b>Get:</b> This button can be used to get the current operational state from the NE.</p> <p>The <b>Apply</b> button is used to confirm the changes in the V5.2 Interface Data field.</p>
<b>Command buttons</b>	<p>The <b>V5 User Ports...</b> button provides access to the <i>V5 User Port List</i> window, limited to the user ports that are linked to this V5 Interface.</p> <p>The <b>Add PSTN...</b> button provides access to the <i>V5 User Port PSTN</i> window, where the V5.2 Interface is populated (and cannot be modified).</p> <p>The <b>Add ISDN...</b> button provides access to the <i>V5 User Port ISDN-BRA</i> window, where the V5.2 Interface is populated (and cannot be modified).</p> <p>The <b>V5 Links...</b> button provides access to the <i>V5.2 Add/Remove Links</i> window.</p> <p>The <b>Signalling...</b> button provides access to the <i>V5 Signalling</i> window for this V5.2 Interface.</p> <p>The <b>Protection...</b> button provides access to the <i>V5.2 Group 2 Protection</i> window for this V5.2 Interface.</p>

Parameters/ Buttons	Description
<b>Primary Link</b>	<p>If a primary feeder is not yet configured all fields remain empty except the field <b>Configuration State</b>.</p> <p>The <b>Physical Feeder</b> shows the id that is configured as primary feeder, if there is one.</p> <p>The <b>V5 Link id</b> shows the link id that is configured as primary feeder, if there is one. Possible values: {0, 255}.</p> <p>The <b>CC id</b> shows the id of the communication channel that is cross-connected to timeslot 16 of the primary feeder, if there is one. Possible values: {0, 65503}.</p> <p>The field <b>Configuration State</b> indicates whether the primary link is correctly configured or not. Possible values: Not Configured, Partially Configured, Configured.</p> <p>The <b>Set Primary</b> button provides access to the <i>Primary Link</i> window. It is enabled only when the <b>Administrative State</b> is "Locked" and the <b>Configuration State</b> for the primary link and the secondary link is "Not Configured".</p> <p>The <b>Remove Primary</b> button can be used to delete the primary link. It is enabled only when the <b>Administrative State</b> is "Locked" and the <b>Configuration State</b> for the primary link is "Partially Configured" or "Configured" and the <b>Configuration State</b> for the secondary link is "Not Configured".</p>
<b>Secondary Link</b>	<p>If a secondary feeder is not yet configured all fields remain empty except the field <b>Configuration State</b>.</p> <p>The <b>Physical Feeder</b> shows the id that is configured as secondary feeder, if there is one.</p> <p>The <b>V5 Link id</b> shows the id that is configured as secondary feeder, if there is one.</p> <p>The field <b>Configuration State</b> indicates whether the primary link is correctly configured or not. Possible values: Not Configured, Partially Configured, Configured.</p> <p>The <b>Set Secondary</b> button provides access to the <i>Secondary Link</i> window. It is enabled only when the <b>Administrative State</b> is "Locked" and the <b>Configuration State</b> for the primary link is "Configured" and the <b>Configuration State</b> for the secondary link is "Not Configured".</p> <p>The <b>Remove Secondary</b> button can be used to delete the secondary link. It is enabled only when the <b>Administrative State</b> is "Locked" and the <b>Configuration State</b> for the secondary link is "Partially Configured" or "Configured".</p>

If you want to ...	then ...
edit the V5 Interface parameters	change the parameters in the field <b>V5 Interface</b> and click on <b>Apply</b> to confirm. If the administrative state has been changed from "Unlocked" to "Locked" a Warning window pops up:  <b>Changing the administrative state of V5 Interface id may be service affecting. Do you want to continue?</b>
edit a V5.2 User Port	click on <b>V5 User Ports....</b> The <i>V5 User Port List</i> window pops up (cf. Figure 5-41, page 5-115).
add a V5.2 User Port PSTN	click on <b>Add PSTN....</b> The <i>V5 PSTN User Port</i> window pops up (cf. Chapter 5.4.5.1, page 5-118).
add a V5.2 User Port ISDN-BRA	click on <b>Add ISDN....</b> The <i>V5 ISDN-BRA User Port</i> window pops up (cf. Chapter 5.4.5.2, page 5-124).
add a V5.2 Link	click on <b>V5 Links....</b> The <i>V5.2 Add/Remove Link</i> window pop up (cf. Chapter 5.4.2.2, page 5-96).
modify the signalling parameters	click on <b>Signalling....</b> The <i>V5 Signalling</i> window pops up (cf. Chapter 5.4.6).
modify the group 2 protection	click on <b>Protection....</b> The <i>V5.2 Group 2 Protection</i> window pops up (cf. Chapter 5.4.6.7).
set a primary Link	click on <b>Set Primary...</b> in the <b>Primary Link</b> field. The <i>Primary Link</i> window pops up (cf. Chapter 5.4.3, page 5-109)
remove a primary link	click on <b>Remove Primary.</b> (cf. Chapter 5.4.14, page 5-157)
set a secondary link	click on <b>Set Secondary...</b> in the <b>Secondary Link</b> field. The <i>Secondary Link</i> window pops up (cf. Chapter 5.4.4, page 5-111)
remove a secondary link	click on <b>Remove Secondary.</b> (cf. Chapter 5.4.15, page 5-158).
exit the window	click on <b>Close.</b>

## 5.4.2 Add V5 Links to V5 Interface

This Section is divided in two subsections:

- V5.1 Set Feeder
- V5.2 Add Link.

### Assumptions

To add a V5 Link to a V5 Interface the following assumptions must be fulfilled:

- The NE is connected.
- The V5 Interface administrative primary service state is OOS (Out of Service) (only for V5.1).
- The physical feeder is not used by any other V5 Interface or leased line link.
- The V5 Link identifier must be unique within the V5 Interface (only for v5.2).

### 5.4.2.1 Add a V5.1 Feeder

#### Procedure

Complete the following procedure to add a link to the V5.1 Interface (only one link is possible).

Step	Procedure
------	-----------

- |    |  |
|----|--|
| 1. | Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Add/Remove Links</b> via the cursor menu or select <b>Service -&gt; Provisioning -&gt; Add/Remove Link</b> via the menu bar. The <i>V5.1 Set Feeder</i> window pops up. |
|----|--|

This window can also be reached from the *V5.1 Interface* window by clicking on **Set Feeder...** (cf. Chapter 5.4.1.1, page 5-87).

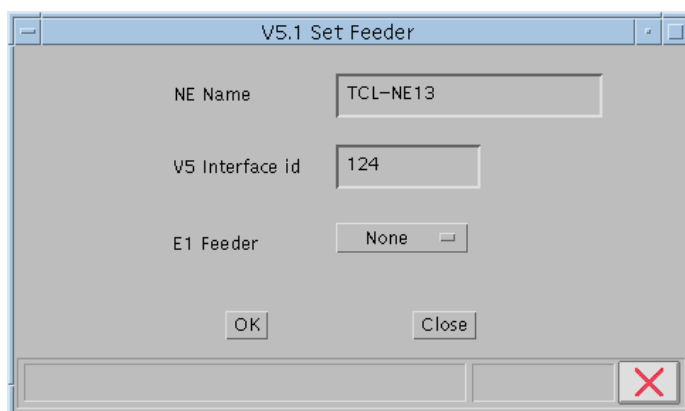



Figure 5-34 "V5.1 Set Feeder" Window

Parameters/ Buttons	Description
<b>E1 Feeder</b>	<p>This option menu can be used to select the desired feeder. It shows the list of physical feeders that are not linked to V5 Interfaces (i.e. they are not related to V5 Links which are cross-connected with V5 Interfaces) or used in leased line groups.</p> <p>Format: e1-shelf-slot-feeder. Possible values: e1-1-{1, 4}-{1, 4}.</p>
<b>OK</b>	<p>This button can be used to set the cross-connection between the V5 Interface and the selected feeder.</p> <p>If the selected feeder has no V5 Link associated, the <i>E1 Feeder/V5 Link</i> window (tab Cross-Connection) pops up for that physical feeder.</p>

2. Use the option menu **Physical Feeder** to select an appropriate feeder.
3. Click on **OK** to confirm the selection. The *E1 Feeder/V5 Link* window pops up (tab Cross-connection - cf. Chapter 5.4.2.4.1, page 5-101) to create the link in a way that cross-connecting is possible. After that the *V5.1 Set Feeder* window is available again and the V5 Link and the related cross-connection will be added. In additional
  - V5 communication path (CP) *Control*
  - V5 communication channel (CC)
  - Cross-connection between CP *Control* and CC
  - Cross-connection between CC and V5 Link's timeslot 16
 will be added.

 **NOTE:**  
A V5.1 link can be created by setting a V5.1 Feeder and then cross-connect it to a V5.1 Interface.

5.4.2.2 Add a V5.2 Link

This window displays the current feeder status of the V5.2 Interface and provides the opportunity of modification.

**Procedure** Complete the following procedure to add a link (links) to the V5.2 Interface. Up to 16 V5.2 Links are possible.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Add/Remove Links</b> via the cursor menu or select <b>Service -&gt; Provisioning -&gt; Add/Remove Link</b> via the menu bar. The <i>V5.2 Add/Remove Links</i> window pops up.  This window can also be reached from the <i>V5.2 Interface</i> window by clicking on <b>V5 Links...</b> (cf. Chapter 5.4.1.2, page 5-90).

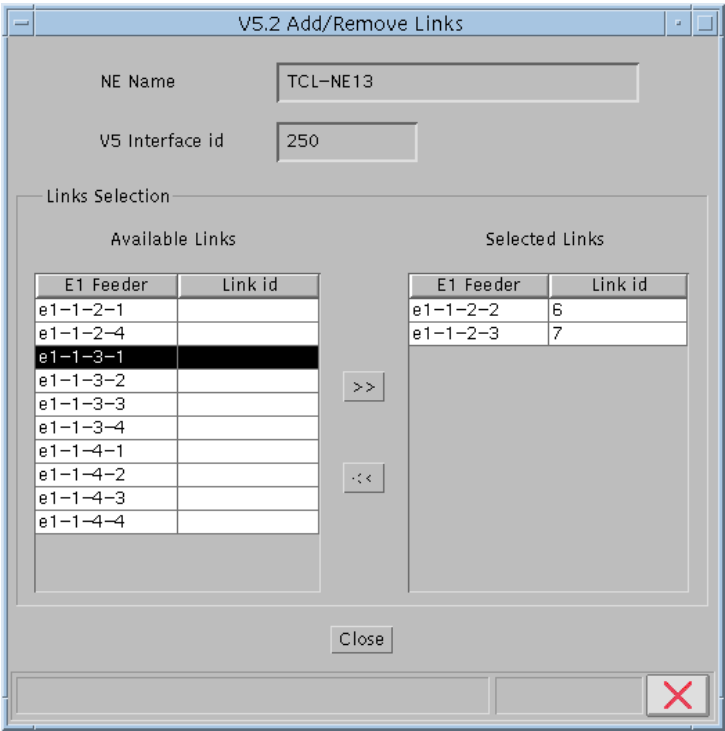


Figure 5-35 "V5.2 Add/Remove Link" Window

The following table shows the view/edit options of the *V5.2 Add/Remove Links* window:

Parameters/ Buttons	Description
<b>Links Selection</b>	<p>This field is subdivided in two parts:</p> <p><b>Available Links</b> and <b>Selected Links</b>.</p> <p>The <b>Available Links</b> list contains all the feeders that are neither associated to a V5 link which is cross connected to a V5 Interface, nor used in a leased line group. Selecting a row in this list activates the <b>Add (&gt;&gt;)</b> button (see below).</p> <p>The <b>Selected Links</b> list contains all the links that are cross-connected to this V5 Interface. Selecting a row in this list activates the <b>Remove (&lt;&lt;)</b> button (see below).</p> <p><b>Feeder:</b> Identifies the physical feeder. Double clicking on any row of either table (available or selected links) opens the <i>E1 Feeder/V5 Link</i> window (V5 Link tab).</p> <p><b>Link id:</b> Shows the link id of the corresponding feeder. If a V5 Link is not yet available this field is empty.</p>
<b>Add (&gt;&gt;)</b>	<p>This button is used to add a link to the V5.2 Interface (cross-connection). It is active only if a feeder in the <b>Available Links</b> list has been selected.</p> <p>If the feeder already carries a V5 Link, and the <b>Link id</b> is not present in the V5.2 Interface yet, the feeder will be cross-connected to the V5.2 Interface (if the <b>Link id</b> is already in use in this V5.2 Interface the command will be rejected).</p> <p>In case the V5 Link is not yet defined, the <i>E1 Feeder/V5 Link</i> window (Cross-Connection tab) pops up (cf. Chapter 5.4.2.4.1, page 5-101) for that link, permitting the modification of the link in a way that cross-connecting is possible. The <i>V5.2 Add/Remove Links</i> window is locked until the <i>E1 Feeder/V5 Link</i> window will be closed. After that the value of the V5 Link id is checked.</p> <p>If this is a valid value and the number of V5 links cross connected to the V5.2 interface is less or equal than 16, the feeder will be cross-connected.</p> <p>If not, it remains in the available list, and the cross-connection operation is cancelled. Modification(s) in the <i>E1 Feeder/V5 Link</i> window can not be cancelled.</p>
<b>Remove (&lt;&lt;)</b>	<p>This button is active only if a feeder in the <b>Selected Links</b> list has been selected. It is used to remove a cross-connection between a V5 Link and the V5.2 Interface.</p> <p>If the V5 Interface is unlocked, and the selected feeder is the primary or secondary feeder (protection group 1 - cf. Chapter 5.4.3, page 5-109), the remove function is not available.</p>

2. Select an appropriate feeder in the **Available Links** list and click on **Add (>>)** or double click on the feeder. The *E1 Feeder/V5 Link* window (V5 Link tab) pops up to modify the link in a way that cross- connecting is possible (cf. Chapter 5.4.2.4.2, page 5-104). After that the *V5.2 Add/Remove Link* window is available again and the V5 Link and the related cross-connection will be added.
3. Repeat step 2 to add another **Available Link(s)** or proceed with step 4.
4. Click on **Close** to exit the window.



### 5.4.2.3 Configure E1 Feeder List

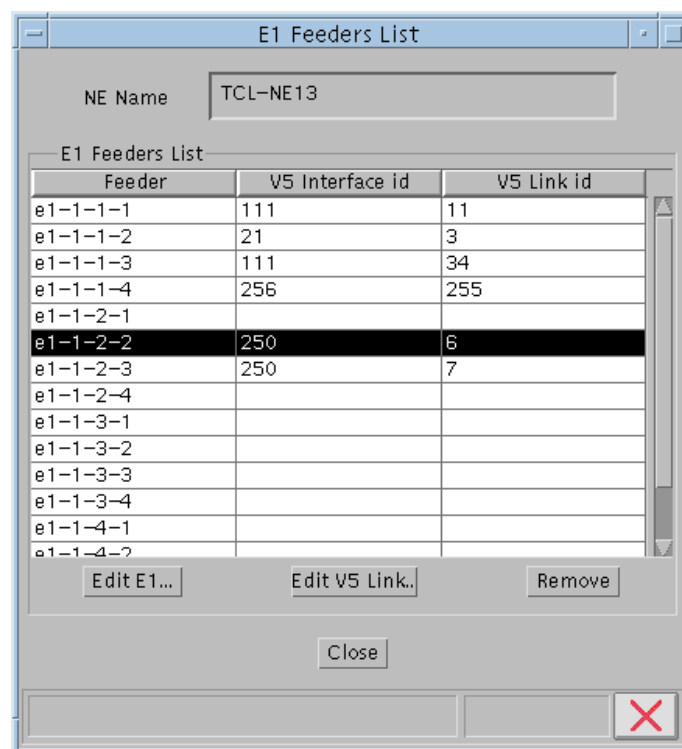
This window shows all available E1 feeders and provides access to E1 Feeder/V5 *Link* window for link parameter modification and for feeder information.

#### Procedure

Complete the following procedure to edit the *E1 Feeders List*.

Step	Procedure
------	-----------

- |    |  |
|----|--|
| 1. | Select <b>All -&gt; NE -&gt; E1 Feeders List</b> in the Network Browser and <b>Edit</b> via the cursor menu<br>or select <b>File -&gt; Open</b> or <b>Service -&gt; Provisioning -&gt; Edit/View</b> via the menu bar. The <i>E1 Feeder List</i> window pops up. |
|----|--|



**Figure 5-36 "E1 Feeders List" Window**

The following table shows the view/edit options of the *E1 Feeders List* window:

Parameters/ Buttons	Description
<b>E1 Feeders List</b>	<p>This scrolling list contains E1 feeders related to the NE. Selecting a row enables <b>Edit</b> and <b>Label...</b> buttons (see below).</p> <p><b>E1 Feeder:</b> Displays the id of the physical feeders.</p> <p><b>V5 Interface id:</b> If the E1 feeder is associated with a V5 Link and the V5 Link is cross-connected to a V5 Interface, the value if the V5 Interface id is displayed here. Possible values: {0, 16777215}. If there is no cross-connection or the V5 Link is not available the value is left empty. If the feeder is in use by a permanent leased line group "Leased" is displayed.</p> <p><b>V5 Link id:</b> Indicates the value of the V5 Link id, if applicable. If this feeder has no associated V5 Link id, the field is left empty. Possible values: {0, 255}. If the feeder is in use by a permanent leased line group "Leased" is displayed.</p>
<b>Command Buttons</b>	<p>In case the feeder is used for leased lines only the <b>Edit E1...</b> button is available.</p> <p><b>Edit E1...:</b> This button is available only if a row in the table is selected. It provides access to the <i>E1 Feeder/V5 Link</i> window.</p> <p><b>Label...:</b> Once a row in the table is selected, this button is available for one of the following cases:</p> <ul style="list-style-type: none"> <li>■ The E1 feeder has a V5 Link already associated. In this case the button is labelled <b>Edit V5 Link...</b> and provides access to the <i>E1 Feeder/V5 Link</i> window.</li> <li>■ The E1 feeder has no V5 Link associated. In this case the button is labelled <b>Add V5 Link...</b> and provides access to the <i>E1 Feeder/V5 Link</i> window.</li> </ul> <p><b>Remove:</b> This button can be used to remove a selected V5 Link. It is available only if there is a V5 Link associated to the E1 feeder.</p>

If you want to ...	then ...
edit an E1 feeder	select an appropriate entry in the list and click on <b>Edit E1...</b> or double click on the feeder. The <i>E1 Feeder/V5 Link</i> window (E1 Feeder tab) pops up (cf. Chapter 5.4.2.4.1, page 5-101).
edit an already associated V5 Link	select an appropriate entry in the list and click on <b>Edit V5 Link...</b> . The <i>E1 Feeder/V5 Link</i> window (V5 Link tab) pops up (cf. Chapter 5.4.2.4.2, page 5-104).
add a V5 Link	select an appropriate entry in the list and click on <b>Add V5 Link...</b> . The <i>E1 Feeder/V5 Link</i> window (Cross-Connection tab) pops up (cf. Chapter 5.4.2.4.2, page 5-104).
remove a V5 Link	select the desired entry and click on <b>Remove</b> . (cf. Chapter 5.4.11, page 5-155).
exit the window	click on <b>Close</b> .

#### 5.4.2.4 Configure E1 Feeder/V5 Link

This window provides physical and logical information of individual feeders and V5 Links. It is subdivided in three tabs: *Cross-Connection*, *Physical Feeder* and *V5 Link*. Tab *V5 Link* is available only if there is a V5 Link already associated to the physical feeder.

##### 5.4.2.4.1 Create a V5 Link

#### Procedure

Complete the following procedure to edit the cross-connection data for creating a V5 Link:

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select <b>All -&gt; NE -&gt; Shelf -&gt; FAC500 -&gt; E1 Feeder</b> in the Network Browser and <b>Create V5 Link</b> via the cursor menu or select <b>Service -&gt; Provisioning -&gt; Create V5 Link</b> via the menu bar. The <i>E1 Feeder/V5 Link</i> window (tab Cross-Connection) pops up. |
|----|---|

This window can also be reached from the *IO\_E1* window (cf. Chapter 5.3.2.1.1, page 5-26) or from the *E1 Feeder List* window (cf. Chapter 5.4.2.3, page 5-99) by clicking on **Add V5 Link...**, from the *Add/Remove V5.2 Link* window (**Add>>**, cf. Chapter 5.4.2.2, page 5-96) or from the *V5.1 Set Feeder* window (**OK**, cf. Chapter 5.4.2.1, page 5-94).

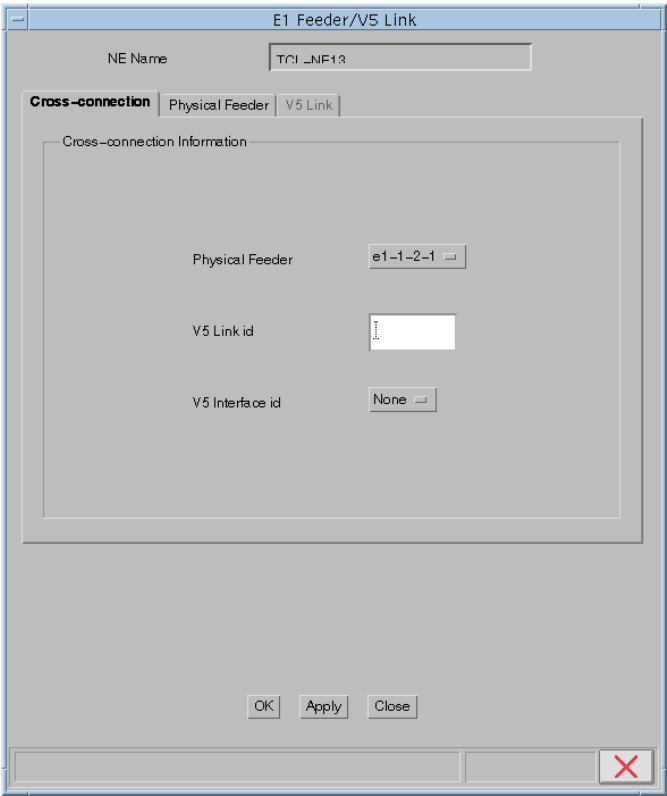


Figure 5-37 "E1 Feeder/V5 Link" Window (Tab Cross-Connection)

The following table shows the options of the cross-connection parameters:

Parameters/ Buttons	Description
<b>Cross-Connec- tion</b>	<p><b>Physical Feeder:</b> This option menu is used to select the specific E1 feeder to the V5 Link to be created. The list shows all free E1 feeders present in the shelf (not yet cross-connected to another V5 Link or carrying a leased line service) or None if there are no free E1s in the NE.</p> <p>Format: e1-shelf-slot-feeder. Possible values: e1-1-{1, 4}-{1, 4}.</p> <p>If this tab is invoked via Network Browser or from windows in which the E1 feeder has been selected this field shows the previously selected feeder.</p> <p>If this tab is invoked from the tab <i>E1 Feeder</i> this field shows the previously selected E1 if it is free; otherwise it shows the first free E1 feeder (if there are no free E1s None value is shown).</p> <p>If this tab is invoked from the tab <i>V5 Link</i> this field shows the first free E1 feeder (if there are no free E1s None value is shown).</p> <p><b>V5 Link id:</b> This field is used to enter the V5 Link id of the V5 Link to be created.</p> <p>Possible values: {0, 255}.</p> <p>If only None is available (there are no free E1s) this field is not editable.</p> <p><b>V5 Interface id:</b> This option menu is used to select a V5 Interface to cross-connect with the V5 Link when this is created.</p> <p>Possible values: {0, 16777215}.</p> <p>If this tab is invoked from <i>V5.2 Add/Remove Link</i> or <i>V5.1 Set Feeder</i> the previously selected value is shown.</p> <p>If there are no V5 Interfaces created "None" is shown.</p>
<b>Command But- tons</b>	<p><b>OK:</b> This button is used to create a V5 Link (with default values and cross-connected to a V5 interface if applicable) and to close the whole window.</p> <p><b>Apply:</b> This button is used to create a V5 Link (with default values and cross-connected to a V5 interface if applicable) and to open the <i>V5 Link</i> tab to be able to change any of its parameters.</p>

2. Use the option menu **Physical Feeder** to select an appropriate E1 feeder.
3. Enter a **V5 Link id** as prerequisite for adding a V5 Link.

4. Use the option menu **V5 Interface id** to select a V5 Interface (this step is optional).
5. Press **OK** to confirm and to close the whole window or press **Apply** to confirm and to open tab V5 Link for modification (cf. Chapter 5.4.2.4.2, page 5-104).

**NOTE:**

The tab Physical Feeder is described in Chapter 5.3.2.1.2, page 5-29.

#### 5.4.2.4.2 Edit V5 Link

This window displays the V5 Link information. This tab is not accessible if there is no V5 Link associated to the E1 feeder.

**Procedure**

Complete the following procedure to view/edit the V5 Link data:

---

Step	Procedure
------	-----------

---

1. Select **All -> NE -> Shelf -> FAC500 -> E1 Feeder** in the Network Browser and **Edit** via the cursor menu or select **Service -> Provisioning -> Edit** via the menu bar. The *E1 Feeder/V5 Link* window (tab E1 Feeder) pops up.

2. Select tab V5 Link.

This window can also be reached from the *E1 Feeders List* window (cf. Chapter 5.4.2.3, page 5-99) or from the IO\_E1 window (cf. Chapter 5.3.2.1.1, page 5-26) by clicking on **Edit V5 Link...**

**NOTE:**

This tab is only accessible if a V5 Link is already associated to the E1 feeder.

**E1 Feeder/V5 Link**

NE Name:

Tab: Cross-connection | Physical Feeder | **V5 Link**

**V5 Link**

Physical Feeder:

V5 Link id:

Administrative State:

V5 Interface id:

**Service Degradation**

Near End:    Far End:

**Communication Channels**

Timeslot	Channel Type	CC id
15	B	
31	B	
16	C	5

**Service State**

Operational State:


**Figure 5-38 "E1 Feeder/V5 Link" Window (Tab V5 Link)**

**NOTE:**  
The parameters in this window can only be modified if the administrative state is "Locked".

The following table shows the options of the V5 Link parameters:

Parameters/ Buttons	Description
<b>V5 Link Data</b>	<p><b>Physical Feeder:</b> Displays the physical feeder selected in the previous window.</p> <p>Format: e1-shelf-slot-feeder. Possible values: e1-1-{1, 4}-{1, 4}.</p> <p><b>V5 Link id:</b> This field is only editable when not cross-connected to a V5 Interface or when cross-connected to a V5 Interface that is "Locked" (see below).</p> <p>Possible values: {0, 255}.</p> <p><b>Remove:</b> This button can be used to remove the current V5 Link.</p> <p><b>Administrative State:</b> This option menu offers four possible values: Locked, Shutdown (Non Deferred), Shutdown (Deferred), Unlocked.</p> <p>The values "Shutdown" are only available when the current state is "Unlocked" and the link is cross-connected to a V5 Interface.</p> <p>When the value is "Unlocked" or "Shutdown" none of the V5 Link parameters can be modified (i.e. the components of the window are disabled).</p> <p><b>V5 Interface id:</b> This option menu indicates the V5 Interface id the link is cross-connected to.</p> <p>Possible values: The existing V5 Interface id (except for V5.1 Interfaces that already have a link cross-connected), None.</p> <p>"None" is used for removing the cross-connection between the V5 Link and the interface.</p>
<b>Service Degradation</b>	<p><b>Near End:</b> This slider can be used to define the threshold value for the near end bit error ratio detection on the related E1 feeder.</p> <p>Possible values: {-7, -4}, step 1.</p> <p><b>Far End:</b> This slider can be used to define the threshold value for the far end bit error ratio detection on the related E1 feeder.</p> <p>Possible values: {-7, -4}, step 1.</p>



Parameters/ Buttons	Description
<b>Communication Channels</b>	<p>The information in this table is only available if there is a V5 Interface cross-connected. The first column contains the timeslot id, the second the channel type, the third the communication channel id if a communication channel is cross-connected. There are three rows, one for timeslot 16, one for timeslot 31 and one for timeslot 15, in that order.</p> <p>The values in this field cannot be edited here, but only via the <i>V5 Signalling</i> window (cf. Chapter 5.4.6, page 5-132).</p> <p><b>Timeslot:</b> Displays a timeslot of 64 kbit/s within the 2.048 Mbit/s V5 Link.</p> <p>Possible values: 16, 31, 15.</p> <p>These are fixed values, are ordered at this way because of the assignment order in V5.</p> <p><b>Channel Type:</b> Possible values: "B", "C".</p> <p>Bearer channels (B) are used to transport bearer information. Communication channels (C) are used to transport all other information.</p> <p>All V5 timeslots are initially provisioned for bearer service (B).</p> <p><b>CC ID:</b> Displays the identifier of the cross-connected communication channel.</p> <p>There is no value if the type of channel is "B" type, nor if there is no communication channel cross-connected.</p> <p>Possible values: {0, 65503}.</p> <p> <b>NOTE:</b> Although 65503 is the maximum value, only 3 communication channels can exist for a V5.1 Interface; and 47 for a V5.2 Interface.</p>
<b>Operational State</b>	<p><b>Service State:</b> Displays the operational state of the V5 Link.</p> <p>Possible values are: Enabled, Disabled.</p> <p><b>Get:</b> This button can be used to obtain the operational state from the NE.</p>
<b>Apply</b>	This button applies the changes made.

3. Define the parameters in the **V5 Link Data** field.
4. Define the parameters in the **Service Degradation** field.
5. Click on **Apply** to confirm.

If the V5 Interface id was entered, the link will be cross-connected, if the link id is unique within the V5 Interface (V5.2 only) (Cross-connect a V5 link).

If the V5 Interface id was modified to "None", the link is removed from that interface. This is legal in certain cases only, that will be checked by the NE. In this case a warning message is displayed before executing the operation (delete cross-connection between interface and link).

**Removing cross-connection between V5 Link id and V5 Interface id may be service affecting. Do you want to continue?**

6. Click on **Close** to exit the window.

### 5.4.3 Add Primary V5.2 Links

#### Protection Groups

A V5.2 Interface supports two protection groups:

- Protection Group 1  
which is handled by setting the primary feeder and secondary feeder (cf. this section and Chapter 5.4.4, page 5-111).  
If the primary feeder becomes faulty a protection switch to the secondary feeder takes place.
- Protection Group 2  
which can have up to 43 working communication channels protected and up to three standby timeslots. The handling of protection group 2 is described in Chapter 5.4.6.7, page 5-146.



NOTE:

Only a primary link can be cross-connected to a communication channel.



NOTE:

Protection switching is possible only for V5.2 protocol.

#### Window

The *Primary Link* window displays the V5 primary link information. The primary link configuration of a V5.2 Interface identifies the V5 Link and the V5 communication channel that are selected to carry the signalling which is not related to on-demand services (Control, Link Control and BCC protocol).

This window can only be reached from the *V5.2 Interface* window (cf. Chapter 5.4.1.2, page 5-90) by clicking on **Set Primary...**

Primary Link

NE Name: TCL-NE14

V5 Interface id: 224

Available Links Selection

Physical Feeder	V5 Link id
e1-1-1-1	6
e1-1-2-4	23
e1-1-3-1	19

Primary Link id: 23

CC id:

OK Close

**Figure 5-39 "Primary Link" Window**

The following table shows the view/edit options of the *Primary Link* window:

Parameters/ Buttons	Description
<b>Primary Link Selection</b>	<p>This list contains all the links that are cross-connected to this V5 Interface.</p> <p><b>E1 Feeder:</b> Displays physical address of the E1 feeders.</p> <p>Format: e1-shelf-slot-feeder.</p> <p>Possible values: e1-{1}-{1, 4}-{1, 4}.</p> <p><b>V5 Link id:</b> This list contains all the links that are cross-connected to this V5 Interface.</p> <p>Possible values: {1, 255}.</p>
<b>Primary Link id</b>	<p>This value corresponds either to the current primary feeder link id, or to the selected item in the available links list, or is empty in case there is no valid primary feeder configured and no selection was made.</p> <p>Possible values: {1, 255}.</p>

Parameters/ Buttons	Description
<b>CC id</b>	<p>This field shows either the id of the current communication channel (CC) used for the primary feeder, or empty if no correctly configured CC is available, or the value the user has entered.</p> <p>Possible values:{0, 65503}.</p> <p>⇒ <b>NOTE:</b> Although 65503 is the maximum value, only 47 communication channels can exist for a V5.2 Interface.</p>
<b>OK</b>	<p>This button is available only if a change was made, i.e. either a CC id was entered, or a feeder was selected, or both. It will use the current data to modify the configuration such that the selected feeder and CC id will identify the primary feeder.</p>

**Procedure**

Complete the following procedure to edit/view a primary link.

Step	Procedure
1.	Select an appropriate feeder in the <b>Primary Link Selection</b> list.
2.	Enter/change the <b>CC id</b> .
3.	Click on <b>OK</b> to confirm or click on <b>Close</b> to exit the window without action.

⇒ **NOTE:**  
When a primary link is created the following entities are automatically created: time slot 16 is set to CC type, a CC with the defined CC id is created and cross-connected to that slot, communication paths *Control*, *Link Control* and *BCC* are created and cross-connected to that CC.

#### 5.4.4 Add Secondary V5.2 Link

This window displays V5 secondary link information. The secondary link configuration of a V5.2 Interface identifies the V5 Link that is selected to carry the protection group number 1 (protection protocol).

⇒ **NOTE:**  
The configuration of a secondary link is only possible if a primary link is already configured.

The *Secondary Link* window can only be reached from the *V5.2 Interface* window (cf. Chapter 5.4.1.2, page 5-90) by clicking on **Set Secondary...**

**Figure 5-40 "Secondary Link" Window**

The following table shows the view/edit options of the *Secondary Link* window:

Parameters/ Buttons	Description
<b>Secondary Link Selection</b>	<p>This list contains all the links that are cross-connected to this V5 Interface, except the one that is configured as primary link.</p> <p><b>E1 Feeder:</b> Displays physical address of the E1 feeders. Format: e1-shelf-slot-feeder. Possible values: e1-{1}-{1, 4}-{1, 4}.</p> <p><b>V5 Link id:</b> This list contains all the links that are cross-connected to this V5 Interface. Possible values: {1, 255}.</p> <p><b>Secondary Link id:</b> This value corresponds either to the current secondary feeder link id, or to the selected item in the available link list, or is empty in case there is no valid secondary feeder configured and no selection was made. Possible values: {1, 255}.</p>
<b>OK</b>	<p>This button is available only if a change was made, i.e. a feeder has been selected. It will use the current data to modify the configuration such that the selected feeder will identify the secondary feeder.</p>

**Procedure**

Complete the following procedure to edit/view a secondary link.

Step	Procedure
1.	Select an appropriate feeder in the <b>Secondary Link Selection</b> list.
2.	Click on <b>OK</b> to confirm or click on <b>Close</b> to exit the window without action.

**NOTE:**

When a secondary link is created the following entities are automatically created: protection group 1, time slot 16 is set to CC type and cross-connected with that protection group, the CC related to primary link in that interface is cross-connected also with that protection group, protection protocol communication path is created and cross-connected with protection group 1.

### 5.4.5 Add V5 User Port

#### Overview

Each V5 User Port can contain a number of V5 User Port bearer channels (64 kbit/s bearer channel CTP (Connection Termination Point)). Each V5 Link contains 32 V5 timeslots (timeslot number 0 is reserved for synchronization purposes) which represent the CTPs corresponding to the physical timeslots which may be configured (a V5 timeslot can be used as bearer channel or as communication-channel). Each V5 User Port bearer channel has to be associated (cross-connected) with a unique V5 timeslot within a V5.1 Interface, but for V5.2 Interfaces the association between V5 User Port bearer channels and V5 timeslots is dynamically controlled by the V5.2 BCC protocol.

#### Assumptions

For the following description it is assumed that

- the NE is connected
- the physical drop is provisioned and is not used for any other V5 User Port or leased line subscriber
- the V5 Layer 3 Port Address (PSTN User Ports) is unique within the V5 Interface
- the Envelope Function Address (ISDN-BRA User Ports) is unique within the V5 Interface
- and the V5 timeslot is configured as bearer channel and is not in use (only for V5.1).

#### Procedure

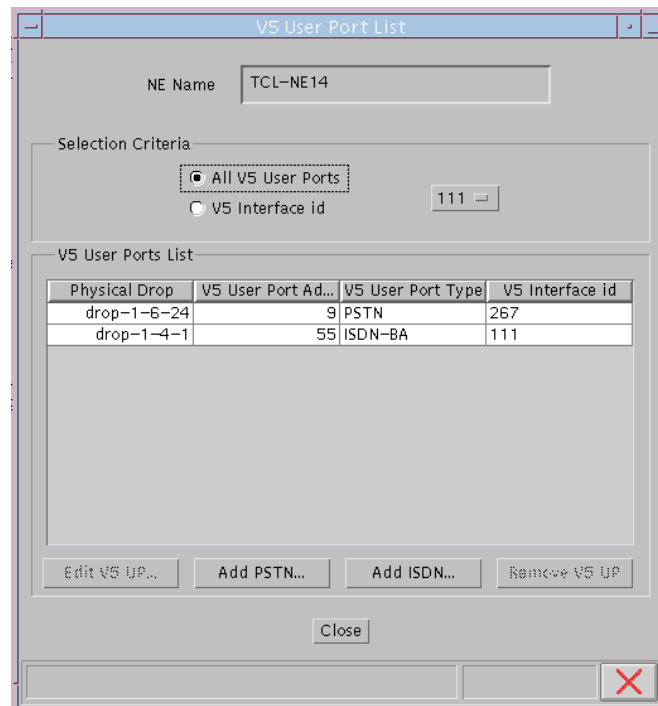
Complete the following procedure to add a V5 User Port.

Step	Procedure
------	-----------

- |    |  |
|----|--|
| 1. | Select <b>All -&gt; NE -&gt; V5 User Port List</b> in the Network Browser and <b>Edit</b> via the cursor menu<br>or select <b>File -&gt; Open</b> or <b>Service -&gt; Provisioning -&gt; Edit</b> via the menu bar. The <i>V5 User Port List</i> window pops up. |
|----|--|

This window can also be reached from the *V5.x Interface* windows (cf. Chapter 5.4.1.1, page 5-87 and Chapter 5.4.1.2, page 5-90) by clicking on **V5 User Ports....**






**Figure 5-41 "V5 User Port List" Window**

This window displays the **V5 User Port List** based on a selection criteria.

Parameters/ Buttons	Description
<b>Selection Criteria</b>	<p>Radio buttons are used to define the list that will be displayed in the table <b>V5 User Ports List</b> (see below).</p> <ul style="list-style-type: none"> <li>■ <b>All V5 User Ports:</b> The list displays all the V5 User Ports (PSTN, ISDN-BRA) currently present in the NE.</li> <li>■ <b>V5 Interface id:</b> If this radio button is selected the list below displays all the V5 User Ports cross-connected with the V5 Interface id selected in the option menu.</li> </ul>

Parameters/ Buttons	Description
<b>V5 User Port List</b>	<p>The information in this field is displayed in a 4-column table:</p> <ul style="list-style-type: none"> <li> <b>Physical Drop:</b> Displays the physical port id associated to the V5 User Port shown in the row.  Format: drop-shelf-slot-port  Possible values: drop-1-{1, 16}-{1, 32}. </li> <li> <b>V5 User Port Address:</b> Indicates the V5 User Port address within the V5 Interface.  Possible values:  {0, 32767} for PSTN User Port (Layer 3 Port Address)  {0, 8175} for ISDN-BRA User Port (Envelope Function Address).  If the drop is used for leased lines "Leased" is displayed. </li> <li> <b>V5 User Port Type:</b> Displays the type of service provided.  Possible values: PSTN, ISDN-BRA.  If the drop is used for leased lines "Leased" is displayed. </li> </ul> <p> <b>NOTE:</b>  PSTN <b>and</b> ISDN-BRA is not possible within the same AP.</p> <ul style="list-style-type: none"> <li> <b>V5 Interface id:</b> Displays the V5 Interface id.  Possible values: {0, 16777215}. </li> </ul>

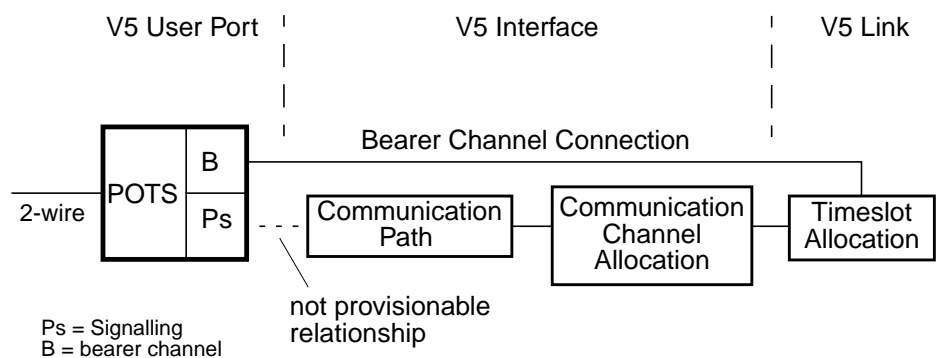
Parameters/ Buttons	Description
<b>Command Buttons</b>	<p>The <b>Edit V5 User Port</b> button is enabled only when a row is selected. It provides access to the <i>V5 (PSTN or ISDN) User Port</i> window to edit the V5 User Port parameters (whenever this is possible) or even create, change or remove cross-connections with other V5 entities: V5 Interface, V5 Communication Paths (ISDN) and V5 Timeslots (V5.1 protocol).</p> <p>The <b>Add PSTN</b> button is enabled when no row is selected. It provides access to the <i>V5 PSTN User Port</i> window (cf. Chapter 5.4.5.1, page 5-118) to provision a new V5 PSTN User Port.</p> <p>The <b>Add ISDN</b> button is enabled when no row is selected. It provides access to the <i>V5 ISDN-BRA User Port</i> window (cf. Chapter 5.4.5.2, page 5-124) to provision a new V5 ISDN-BRA User Port.</p> <p>The <b>Remove V5 User Port</b> button is enabled only when a row is selected. It can be used to delete all the existing cross-connections between V5 User Port and other V5 entities and the V5 User Port entity.</p>

If you want to ...	then ...
add a V5 User Port	click on <b>Add PSTN</b> or <b>Add ISDN</b> . The corresponding window pops up (cf. Chapter 5.4.5.1, page 5-118 for PSTN, cf. Chapter 5.4.5.2, page 5-124 for ISDN-BRA).
edit an already existing V5 User Port	use the radio buttons to choose a desired user port, select an appropriate entry in the list and click on <b>Edit V5 User Port</b> . The corresponding window pops up (cf. Chapter 5.4.5.1, page 5-118 for PSTN, cf. Chapter 5.4.5.2, page 5-124 for ISDN-BRA).
remove an existing V5 User Port	select the desired entry in the list and click on <b>Remove V5 User Port</b> (cf. Chapter 5.4.10, page 5-155).
exit the window	click on <b>Close</b> .

5.4.5.1     **Configure V5 PSTN User Port**

**Overview**                      The PSTN entity represents a PSTN User Port which can be associated to a V5 Interface. It contains only one user port bearer channel.

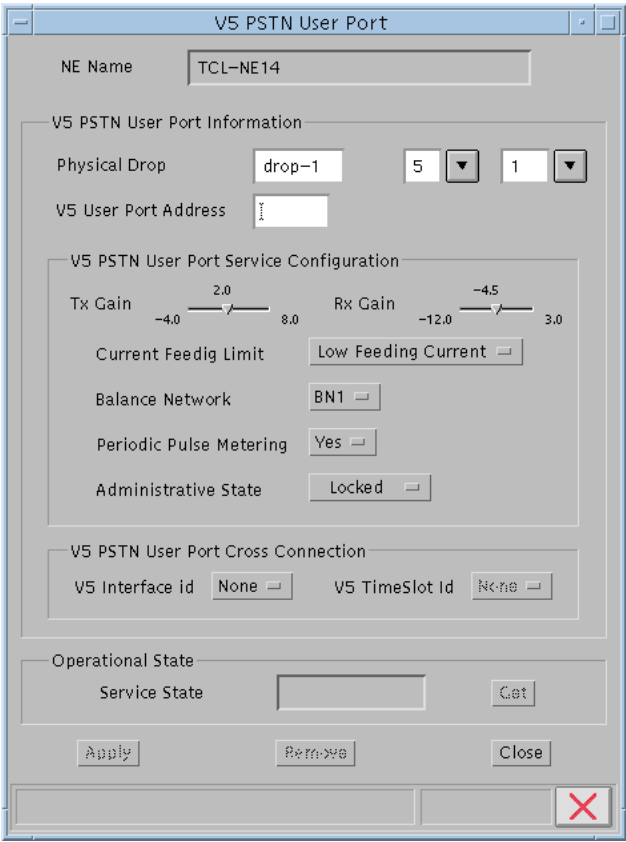
The PSTN protocol information for all the POTS User Ports associated to a specific V5 Interface (V5.1 / V5.2) is carried by the PSTN V5 Communication Path, and no provisioning action is needed for this subscriber information allocation.



**Figure 5-42     Functional Model of PSTN User Port Configuration**

**Procedure**                      Complete the following procedure to configure a V5 PSTN User Port.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; Shelf -&gt; LPZ120 (LPZ100, LPP100) -&gt; Drop id (PSTN)</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Service -&gt; Provisioning -&gt; Edit/View</b> via the menu bar. The <i>V5 PSTN User Port</i> window pops up.  This window can also be reached from the <i>AP</i> windows (cf. Chapter 5.3.2.1.6, page 5-39), from <i>V5.x Interface</i> window (cf. Chapter 5.4.1.1, page 5-87 and Chapter 5.4.1.2, page 5-90) from <i>V5 User Port List</i> window (cf. Figure 5-41, page 5-115).



**Figure 5-43 "V5 PSTN User Port" Window**

This window is used to add a new V5 PSTN User Port, or modify an existing V5 PSTN User Port.

It allows to create/remove the cross-connection between a V5 PSTN User Port and a V5 Interface, to create/change/remove the cross-connection between a V5 PSTN User Port bearer channel and a V5 timeslot (only for V5.1 protocol) as well as V5 PSTN User Port service parameters configuration and modification.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

If a totally new V5 PSTN User Port is created, all parameters can be specified by the user.

If however this window is invoked from windows in which individual parameters have already been specified (such as Physical Drop, V5 User Port Address and V5 Interface id), it is not possible to change these parameters here at all, or only insignificantly.

**NOTE:**

The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
<b>V5 PSTN User Port Information</b>	<p><b>Physical Drop:</b> This field displays the physical port id associated to the V5 PSTN User Port shown in this window by means of three option menus:</p> <ul style="list-style-type: none"> <li>■ The first one contains drop-shelf (for this release this field is always drop-1).</li> <li>■ The second one contains the slot number {1, 16} inside NE.</li> <li>■ The third one contains the drop number inside the slot indicated on the previous list {1, 32}.</li> </ul> <p>Format: drop-shelf-slot-port. Possible values: drop-1-{1, 16}-{1, 32}.</p> <p>When coming from a window where the drop is already defined the corresponding value is displayed and non-editable.</p> <p>Otherwise this field is empty and editable. The behaviour of this fields when creating a V5 User Port is the following:</p> <ol style="list-style-type: none"> <li>1. The value in the first option menu is drop-1.</li> <li>2. The second option menu contains all the slots which has free drops. Selecting any of them updates the content in the third option menu consequently. If there are no slots with free drops the value "None" is displayed.</li> <li>3. The third option menu contains the free drops inside the slot selected in the second option menu. The operator can select any of the free drops. If there are no free drops the value "None" is displayed.</li> </ol> <p><b>V5 User Port Address:</b> This V5 Layer 3 Port Address identifies a V5 PSTN User Port within a V5 Interface.</p> <p>Possible values: {0, 32767}.</p> <p>If the user port is already created and cross-connected to a V5 Interface, the corresponding value is displayed and can not be changed.</p> <p>If the user port is created and not cross-connected the displayed value is editable.</p> <p>In all the other cases this field is empty and editable.</p>

Parameters/ Buttons	Description
<b>V5 PSTN User Port Service Configuration</b>	<p><b>TX Gain:</b> This slider can be used to define the transmit gain in decibel relative to digital reference point. Possible values: {-4, 8}. Step 0.5.</p> <p><b>RX Gain:</b> This slider can be used to define the receive gain in decibel relative to digital reference point. Possible values: {-12, 3}. Step 0.5.</p> <p><b>Current Feeding Limit:</b> This option menu can be used to select a desired Current Feeding Limit. Possible Values: High Feeding Current, Low Feeding Current.</p> <p><b>Balance Network:</b> This option menu can be used to select a desired Balance Network (BN). Possible values: BN1, BN2, BN3, BN4, BN5.</p> <p><b>Periodic Pulse Metering:</b> This option menu can be used to request the periodic pulse metering. Possible values: Yes, No.</p> <p><b>Administrative State:</b> This option menu can be used to define the V5 PSTN User Port administrative state. Possible values: Locked, Unlocked, Shutdown (default value is "Locked" at creation time).</p>

Parameters/ Buttons	Description
<b>V5 PSTN User Port Cross-Connection</b>	<p><b>V5 Interface id:</b> This field displays the V5 Interface id this user port is cross-connected.</p> <p>Possible values: None, {0, 16777215}.</p> <p>When coming from <i>V5 Interface</i> window via <b>Add PSTN</b> this field is non-editable.</p> <p>If the V5 PSTN User Port is cross-connected to a V5 Interface this field is editable allowing to change it only to "None" value for deleting the cross-connection.</p> <p>In all the other cases an option menu with all V5 Interface ids is offered for selection.</p> <p><b>V5 Timeslot id:</b> This field displays the V5 timeslot id cross-connected to the V5 PSTN User Port bearer channel shown in this window.</p> <p>This option menu is available for selection only when the selected V5 Interface id identifies a V5.1 protocol interface which has a V5 Link already cross-connected.</p> <p>Only available timeslots of type "B" are shown, and only for V5.1.</p> <p>Possible values: None, {1, 31}.</p> <p>This option menu is used to create/change/remove (set "None" value) the timeslot cross-connected with the user port bearer channel.</p>
<b>Operational State</b>	<p><b>Service State:</b> Shows the V5 PSTN User Port operational state obtained from the NE through the use of the <b>Get</b> button.</p> <p>Possible values: Enabled, Disabled.</p>
<b>Command Buttons</b>	<p>The <b>Apply</b> button is used to accept the different changes and keeps the window in view for further use.</p> <p>The <b>Remove</b> button can be used to remove a V5 User Port.</p>



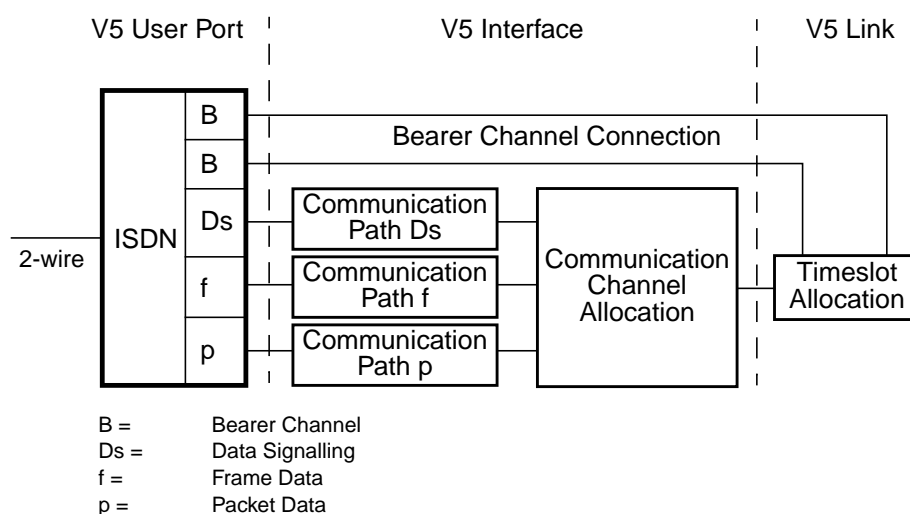
<b>If you want to ...</b>	<b>then ...</b>
add a new V5 PSTN User Port	enter the values for <b>Physical Drop</b> and <b>V5 User Port Address</b> , define the parameters in the <b>V5 PSTN User Port Service Configuration</b> field, use the option menus <b>V5 Interface id</b> and <b>V5 Timeslot id</b> (only for V5.1) to define the desired V5 PSTN cross-connection and click on <b>Apply</b> to confirm.
edit an already existing V5 PSTN User Port and the related options	define the parameters in the <b>V5 PSTN User Port Service Configuration</b> field, use the option menus <b>V5 Interface id</b> and <b>V5 Timeslot id</b> (only for V5.1) to change the V5 PSTN cross-connection and click on <b>Apply</b> to confirm.
remove a cross-connection between a V5 PSTN User Port and the V5 Interface	set the <b>V5 Interface id</b> to "None" and click on <b>Apply</b> to confirm.
remove a cross-connection between a V5 timeslot and the user port bearer channel	set the <b>V5 Timeslot id</b> to "None" and click on <b>Apply</b> to confirm.
remove a V5 User Port	select the corresponding <b>V5 User Port Address</b> and click on <b>Remove</b> . A <i>Warning</i> window pops up:  <b>Removing V5 User Port may be service affecting. Do you want to continue?</b>
exit the window	click on the <b>Close</b> button.

### 5.4.5.2 Configure V5 ISDN-BRA User Port

#### Overview

The ISDN-BRA entity represents an ISDN-BRA User Port which can be associated to a V5 Interface. It contains up to two user port bearer channels (64 kbit/s) for communication signal and a 16 kbit/s D-channel for protocol information.

The ISDN-BRA User Port can have up to three different types of data (data signalling, packet and frame) to be carried over any of the communication channels within the V5 Interface. On the other hand, an ISDN communication path (CP) represents an information type (Ds, p and f) for one or more ISDN-BRA User Ports associated to a V5 Interface.



**Figure 5-44 Functional Model of ISDN-BRA User Port Configuration**

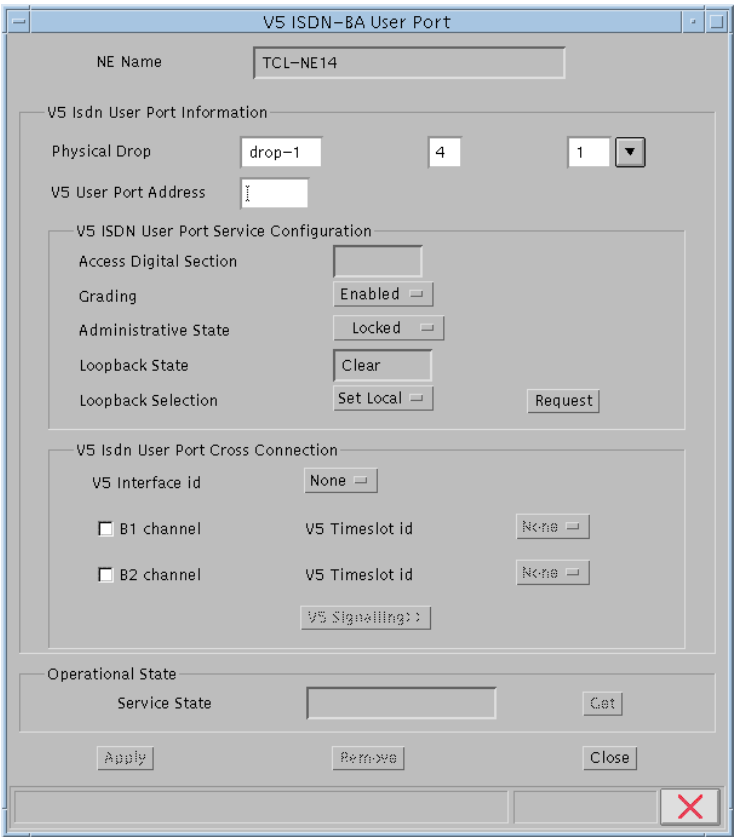
#### Procedure

Complete the following procedure to configure a V5 ISDN-BRA User Port.

Step	Procedure
------	-----------

1. Select **All -> NE -> Shelf -> LPU112 -> Drop id (ISDN)** in the Network Browser and **Edit** via the cursor menu or select **File -> Open** or **Service -> Provisioning -> Edit/View** via the menu bar. The *V5 ISDN-BRA User Port* window pops up.

This window can also be reached from the  
*AP* windows (cf. Chapter 5.3.2.1.6, page 5-39),  
 from *V5.x Interface* window (cf. Chapter 5.4.1.1, page 5-87 and Chapter 5.4.1.2, page 5-90)  
 from *V5 User Port List* window (cf. Figure 5-41, page 5-115).



**Figure 5-45 "V5 ISDN-BRA User Port" Window**

This window is used to add a new V5 ISDN-BRA User Port, remove or modify an existing V5 ISDN-BRA User Port.

It allows to create/remove the cross-connection between a V5 ISDN-BRA User Port and a V5 Interface, to create/change/remove the cross-connection between a V5 ISDN-BRA User Port bearer channel(s) and a V5 timeslot (only for V5.1 protocol), to create/change/remove the cross-connection(s) between a V5 ISDN-BRA User Port and V5 communication path(s) (frame, packet or signalling) as well as V5 ISDN-BRA User Port service parameters configuration and modification.

The following table lists all possible entries/parameters. Whether or not it is possible to edit/change individual parameters depends on the previous actions.

If a totally new V5 ISDN-BRA User Port is created, all parameters can be specified by the user.

If however this window is invoked from windows in which individual parameters have already been specified (such as Physical Drop, V5 User Port Address and

V5 Interface id), it is not possible to change these parameters here at all, or only insignificantly.

**NOTE:**

The parameters in this window can only be modified if the administrative state is "Locked".

Parameters/ Buttons	Description
<b>V5 ISDN User Port Information</b>	<p><b>Physical Drop:</b> This field identifies the physical port id associated to the V5 ISDN-BRA User Port shown in this window by means of three option menus:</p> <ul style="list-style-type: none"> <li>■ The first one contains drop-shelf (for this release this field is always drop-1).</li> <li>■ The second one contains the slot number {1, 16} inside NE.</li> <li>■ The third one contains the drop number inside the slot indicated on the previous list {1, 32}.</li> </ul> <p>Format: drop-shelf-slot-port. Possible values: drop-1-{1, 16}-{1, 32}.</p> <p>When coming from a window where the drop is already defined the corresponding value is displayed and non-editable.</p> <p>Otherwise this field is empty and editable. The behaviour of this fields when creating a V5 User Port is the following:</p> <ol style="list-style-type: none"> <li>1. The value in the first option menu is drop-1.</li> <li>2. The second option menu contains all the slots which has free drops. Selecting any of them updates the content in the third option menu consequently. If there are no slots with free drops the value "None" is displayed.</li> <li>3. The third option menu contains the free drops inside the slot selected in the second option menu. The operator can select any of the free drops. If there are no free drops the value "None" is displayed.</li> </ol> <p><b>V5 User Port Address:</b> This V5 Envelope Function Address identifies a V5 ISDN-BRA User Port within a V5 Interface.</p> <p>Possible values: {0, 8175}.</p> <p>If the user port is already created and cross-connected to a V5 Interface, the corresponding value is displayed and can not be changed.</p> <p>If the user port is created and not cross-connected the displayed value is editable.</p> <p>In all the other cases this field is empty and editable.</p>

Parameters/ Buttons	Description								
<b>V5 ISDN User Port Service Configuration</b>	<p><b>Access Digital Section:</b> This parameter indicates whether or not there is an access digital section at the ISDN-BRA port (present).</p> <p><b>Grading:</b> This option menu can be used to define whether performance measurement grading messages should be sent to the connected LE.</p> <p>Possible values: Enabled, Disabled.</p> <p><b>Administrative State:</b> The option menu can be used to define the administrative state of the User Port.</p> <p>Possible values: Locked, Unlocked, Shutdown (default value is "Locked" at creation time).</p> <p><b>Loopback State:</b> This field displays the current loopback state (Clear or Set). This state can be changed via the <b>Request</b> button on the right hand side (see below).</p> <p><b>Loopback Selection:</b> This option menu is used to define the ISDN-BRA port loopback. It is only enabled if a drop is selected.</p> <p>Possible values:</p> <table> <tr> <td>Set Local</td><td>Loopback switched locally on AP</td></tr> <tr> <td>Set Reg</td><td>Loopback switched at regenerator</td></tr> <tr> <td>Set NT</td><td>Loopback switched at network termination</td></tr> <tr> <td>Clear</td><td>Clear the loopback.</td></tr> </table> <p><b>Request:</b> This button is used to perform the requested operation (option menu Loopback Selection).</p>	Set Local	Loopback switched locally on AP	Set Reg	Loopback switched at regenerator	Set NT	Loopback switched at network termination	Clear	Clear the loopback.
Set Local	Loopback switched locally on AP								
Set Reg	Loopback switched at regenerator								
Set NT	Loopback switched at network termination								
Clear	Clear the loopback.								

Parameters/ Buttons	Description
<b>V5 ISDN User Port Cross-Connection</b>	<p><b>V5 Interface id:</b> This field displays the V5 Interface id this user port is cross-connected.</p> <p>Possible values: None, {0, 16777215}.</p> <p>When coming from <i>V5 Interface</i> window via <b>Add ISDN</b> this field is non-editable.</p> <p>If the V5 ISDN-BRA User Port is cross-connected to a V5 Interface this field is editable allowing to change it only to "None" value for deleting the cross-connection.</p> <p>In all the other cases an option menu with all V5 Interface ids is offered for selection.</p> <p><b>B1 Channel:</b> This check box indicates whether the V5 ISDN-BRA User Port bearer channel 1 shall be used for ISDN data.</p> <p><b>V5 Timeslot id (B1):</b> This field displays the V5 timeslot id cross-connected to the V5 ISDN-BRA User Port bearer channel 1 shown in this window (this field is only available for V5.1).</p> <p>Possible values: None, {1, 31}.</p> <p>This option menu ("None" value is allowed) is available for selection only when the selected V5 Interface id identifies a V5.1 Interface which has a V5 Link already cross-connected and the V5 ISDN-BRA User Port bearer channel 1 is enabled.</p> <p>This option menu is used to create/change/remove (set "None" value) the cross-connection between the bearer channel 1 and the timeslot.</p> <p><b>B2 Channel:</b> This check box indicates whether the V5 ISDN-BRA User Port bearer channel 2 shall be used for ISDN data.</p> <p><b>V5 Timeslot id (B2):</b> This field displays the V5 timeslot id cross-connected to the V5 ISDN-BRA User Port bearer channel 2 shown in this window.</p> <p>Possible values: None, {1, 31}.</p> <p>This option menu ("None" value is allowed) is available for selection only when the selected V5 Interface id identifies a V5.1 Interface which has a V5 Link already cross-connected and the V5 ISDN-BRA User Port bearer channel 2 is enabled.</p> <p>This option menu is used to create/change/remove (set "None" value) the cross-connection between the bearer channel 2 and the timeslot.</p>

Parameters/ Buttons	Description
<b>V5 Signalling &gt;&gt;</b>	<p>This button provides access to the <i>V5 ISDN-BRA User Port Signalling Configuration</i> window where the user is able to create, change or remove cross-connection(s) between V5 ISDN-BRA User Port and V5 ISDN communication path(s) (packet, frame and signalling).</p> <p>This button is available only if the V5 ISDN-BRA User Port is created and cross-connected to a V5 Interface identified in this window by its V5 Interface id.</p>
<b>Operational State</b>	<p><b>Service State:</b> Shows the V5 ISDN-BRA User Port operational state obtained from the NE through the use of the <b>Get</b> button.</p> <p>Possible values: Enabled, Disabled.</p>
<b>Command Buttons</b>	<p><b>Apply:</b> This button is used to accept the different changes and keeps the window in view for further use.</p> <p><b>Remove:</b> This button can be used to remove a V5 User Port.</p>

If you want to ...	then ...
add a new V5 ISDN-BRA User Port	enter the values for <b>Physical Drop</b> and <b>V5 User Port Address</b> , define the parameters in the <b>Service Configuration</b> field, use the option menus <b>V5 Interface id</b> and <b>V5 Timeslot id</b> (only for V5.1) and the check boxes <b>B1 Channel</b> and <b>B2 Channel</b> to define the desired V5 ISDN cross-connection for the bearer channels and click on <b>Apply</b> to confirm.
edit an already existing V5 ISDN-BRA User Port and the related options	define the parameters in the <b>Service Configuration</b> field, use the option menus <b>V5 Interface id</b> and <b>V5 Timeslot id</b> (only for V5.1) and the check boxes <b>B1 Channel</b> and <b>B2 Channel</b> to change the V5 ISDN cross-connection for the bearer channels and click on <b>Apply</b> to confirm.
remove a cross-connection between a bearer channel and timeslot	use the check box ( <b>B1 Channel</b> or <b>B2 Channel</b> ) to select a bearer channel, use the option menu <b>V5 Timeslot id</b> to choose the cross-connected timeslot id (null value) and click on <b>Apply</b> .

If you want to ...	then ...
configure the signalling parameters	click on <b>V5 Signalling &gt;&gt;</b> .
remove a V5 User Port	select the corresponding <b>V5 User Port Address</b> and click on <b>Remove</b> . A <i>Warning</i> window pops up:  <b>Removing V5 User Port may be service affecting. Do you want to continue?</b>
exit the window	click on the <b>Close</b> button.



#### 5.4.5.2.1 V5 ISDN User Port Signalling Configuration

This window is used to configure the V5 ISDN-BRA User Port signalling data. It allows the creating, changing or removing of cross-connection(s) between V5 ISDN-BRA User Port and V5 ISDN communication path(s) (packet, frame and data signalling).

	CP id	CC id
Frame Data Type (F)	27	81
Packet Data Type (P)	33	77
Signalling Data Type (Ds)	31	36

Buttons: Apply, Close, [Red X]

**Figure 5-46 "V5 ISDN User Port Signalling Configuration" Window**

This window displays the V5 communication path ids (frame, packet and signalling) associated to the V5 ISDN-BRA User Port.

The option menus (**CP id**) are available only when the selected V5 Interface id (*V5 ISDN-BRA User Port* window - cf. Chapter 5.4.5.2, page 5-124) identifies a V5 Interface which contains V5 communication path(s) already configured. They display the CPs present in the V5 Interface to which the user port is cross-connected. If no CP is cross-connected "null" value is displayed in this field.

If the selected V5 communication path is already cross-connected to a V5 communication channel, its V5 communication channel id (**CC id**) is also displayed as a non-editable text.

V5 communication path id format:      {0, 9}                      for V5.1 Protocol  
    {0, 146}                      for V5.2 Protocol.

V5 communication channel id format:      {0, 3}                      for V5.1 Protocol  
    {0, 65503}                      for V5.2 Protocol.

The **Apply** button is used to confirm the changes.

The **Close** button can be used to go back to the *V5 ISDN-BRA User Port* window (cf. Chapter 5.4.5.2, page 5-124) to select another user port.

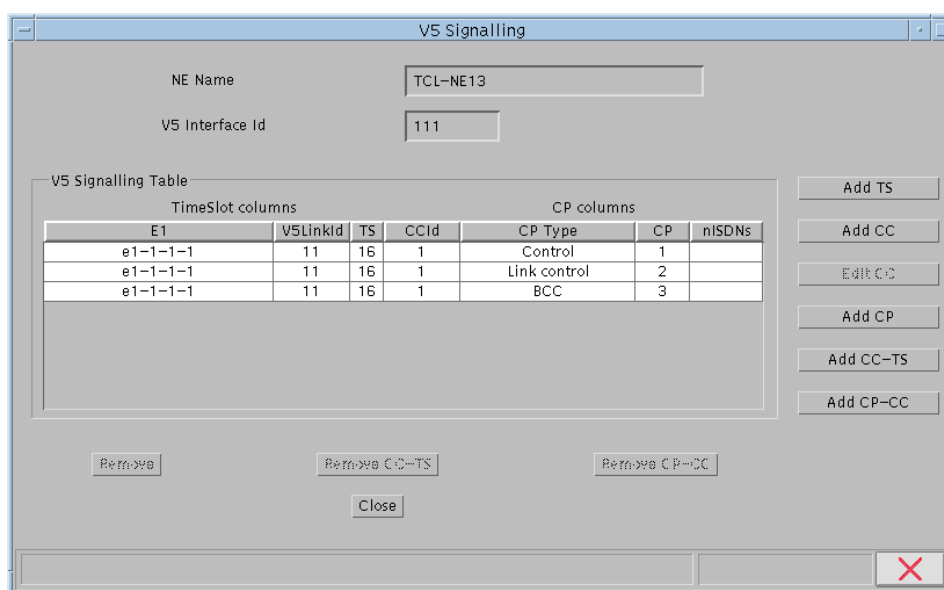
## 5.4.6 V5 Signalling

### Overview

There are several ways to reach this window:

- via *V5.1 Interface* window (cf. Chapter 5.4.1.1, page 5-87)
- via *V5.2 Interface* window (cf. Chapter 5.4.1.2, page 5-90).

This window displays the signalling structure of a V5 Interface. It shows the communication channel time slots (TSs), the communication channels (CCs), communication paths (CPs), links between TS and CC and links between CP and CC. It allows creation, edition and deletion of these.



**Figure 5-47 "V5 Signalling" Window**

### V5 Signalling Table

The V5 Signalling Table consists of 4 fields: Timeslot columns, CC id, CP columns and Number of ISDNs.

Several lines can share a TS and CC, as several CPs can be linked to the same CC (e.g. see below).

Timeslot columns			CP Columns			
		TS	CCId	CP Type	CP	
		15	5	ISDN-D	8	
		15	5	ISDN-f	10	
		15	5	ISDN-p	12	

Absence of an entry (TS, CC or CP) indicates that the link between this entry and the non-absent item does not exist yet. In this cases the **Add...** buttons can be used to establish the desired links.

Each line can be selected separately. Selecting any CP line also selects the related CC and TS fields (if available). Operations allowed on a selection are the delete operations, according to the criteria listed below.

### Protected Items

The protected items are also displayed (group 2 protection). A row that is subject to protection is marked visibly, as not all edition can be performed on it (e.g. different background colour or different text colour). The operations that are not available on these rows are: Remove CC-TS and Add CC-TS. Protections are set and removed from the protection window (cf. Chapter 5.4.6.7, page 5-146).

Parameters/ Buttons	Description
<b>Timeslot columns</b>	<p><b>E1 Feeder:</b> This column contains the physical feeder that carries the concerned time slot.</p> <p>Possible values: e1-{1}-{1, 4}-{1, 4}.</p> <p><b>V5 Link id:</b> This column contains the V5 Link id of the link that is concerned.</p> <p>Possible values: {0, 255}.</p> <p><b>TS:</b> This column contains the time slot number that corresponds to the concerned time slot.</p> <p>Possible values: 15,16,31.</p>
<b>CCid</b>	The entry in this column identifies the communication channel via its CC id.
<b>CP columns</b>	<p><b>CP Type:</b> This column specifies the type of communication path that is concerned.</p> <p>Possible values: Control, Link control (only for V5.2), BCC (only for V5.2), PSTN, ISDN - p, ISDN - f, ISDN - Ds.</p> <p><b>CP:</b> This column specifies an identifier that determines the communication path in a unique way inside the V5 Interface. It is constructed by taking the CP aid, and stripping all except the last number.</p> <p>Possible values: {1, 145}.</p> <p><b>Number of ISDNs:</b> This column specifies, for ISDN communication paths, the number of ISDN-BRA User Ports that are cross-connected to it. It is used only as reference so the user can estimate the importance and traffic on that CP.</p>

Parameters/ Buttons	Description
<b>Command Buttons</b>	<p>The command buttons are only available when the administrative state of the selected V5 Interface is "Locked".</p> <p><b>Add TS:</b> This button provides access to the <i>Add Time Slot</i> window (cf. Chapter 5.4.6.1, page 5-136). The chosen time slot is not created (impossible), but changed to C-channel.</p> <p><b>Add CC:</b> This button provides access to the <i>Add Communication Channel</i> window (cf. Chapter 5.4.6.2, page 5-137).</p> <p><b>Edit CC:</b> This button provides access to the <i>Edit Communication Channel</i> window (modal - cf. Chapter 5.4.6.3). It is only enabled when a row in the table is selected that contains only a TS. This button is only applicable for V5.2.</p> <p><b>Add CP:</b> This button provides access to the <i>Add Communication Path</i> window (cf. Chapter 5.4.6.4, page 5-140).</p> <p><b>Add CC-TS:</b> This button provides access to the <i>Crossconnect Communication Channel with Time Slot</i> window (cf. Chapter 5.4.6.5, page 5-142).</p> <p><b>Add CP-CC:</b> This button provides access to the <i>Crossconnect Communication Path with Communication Channel</i> window (cf. Chapter 5.4.6.6, page 5-144).</p> <p><b>Remove:</b> This button is only enabled when a row in the table is selected that contains only a TS, only a CC or only a CP. The Operation deletes the concerned TS, CC or CP.</p> <p>⇒ <b>NOTE:</b> This button is disabled if the selected TS belongs to a protection group.</p> <p>⇒ <b>NOTE:</b> ISDN CPs can only be deleted if there are no user ports linked to them. These must be deleted from the user port windows.</p> <p>A TS is never really removed, but marked as B-channel (C-channel -&gt; B-channel).</p>

Parameters/ Buttons	Description
<b>Command Buttons</b>	<p><b>Remove CC-TS:</b> This button is only enabled when a row is selected that contains both CC and TS. The operation deletes the cross-connection, after which the row for that TS contains no longer the CC, and the CC is moved to a row without TS.</p> <p>⇒ <b>NOTE:</b> This button is disabled if the selected CC belongs to a protection group.</p> <p><b>Remove CP-CC:</b> This button is only enabled when a row is selected that contains both CP and CC. The operation deletes the cross-connection, after which the row for that CC no longer contains the CP, and the CP is moved to a row without CC.</p>

⇒ **NOTE:**  
This window displays all CPs, CCs and TSs, also those used for the primary and secondary link. The available operations (in the next windows) cannot fully reconstruct a full signalling from scratch, only the ISDN-BRA and PSTN signalling is intended to be managed from this window. The primary and secondary feeder configuration are managed from the primary and secondary feeder subpanes in the *V5.2 Interface* window (cf. Chapter 5.4.1.2, page 5-90).

### 5.4.6.1 Add Time Slot

This modal window is used to allocate a time slot, linked to the V5 Interface to the set of CC time slots. It can be reached only via **Add TS** from the *V5 Signalling* window (cf. Chapter 5.4.6, page 5-132).

E1 Feeder	V5 Link Id	Timeslot
e1-1-1-1	11	15
e1-1-1-1	11	31
e1-1-1-3	34	15
e1-1-1-3	34	16
e1-1-1-3	34	31

**Figure 5-48 "Add Time Slot" Window**

Parameters/ Buttons	Description
<b>Available Time Slots</b>	<p>The scrolling list contains the identification of available time slots for addition to the C-channel list. The list contains only those time slots that are currently B-channel. Candidate time slots are limited to timeslots 15, 16 and 31 of each linked feeder. A single row of this list can be selected.</p> <p><b>E1 Feeder:</b> This column indicates the physical feeder a time slot belongs to.</p> <p><b>V5 Link id:</b> This column contains the V5 Link id of the physical feeder.</p> <p><b>Time Slot:</b> This column shows the number of the time slots within this feeder.</p>
<b>Apply</b>	This button is enabled when a time slot is selected.

**Procedure** Complete the following procedure to add a time slot.

Step	Procedure
------	-----------

- |    |   |
|----|---|
| 1. | Select a row in the <b>Available Time Slots</b> list.                         |
| 2. | Click on <b>Apply</b> . The time slot will be modified to become a C-channel. |
| 3. | Click on <b>Close</b> to exit the window.                                     |

### 5.4.6.2 Add Communication Channel

This modal window is used to create a CC, while creating a CC it can be cross-connected to a time slot (optional). It can be reached only via **Add CC** from the *V5 Signalling* window (cf. Chapter 5.4.6, page 5-132).

**Figure 5-49 "Add Communication Channel" Windows.**

Parameters/ Buttons	Description
<b>Comm. Chan- nel id</b>	This field is used to enter the CC id that shall be created. This value is only taken into account for V5.2  Possible values: {0, 65503}.

Parameters/ Buttons	Description
<b>Available Time Slots</b>	<p>This scrolling list contains the C-channel time slots that are not in the protection mode, and have no CC linked yet.</p> <p><b>E1 Feeder:</b> Displays the physical feeder a time slot belongs to.</p> <p><b>V5 Link id:</b> Displays the V5 Link id associated to the feeder shown in the previous field.</p> <p><b>Timeslot:</b> Displays the CC time slots that are not in the protection mode and have no CC linked yet.</p> <p>Possible values: None, 15, 16, 31.</p>
<b><i>Apply</i></b>	This button is used to create a CC with the given id. It is only enabled when a CC id is specified.

**Procedure**

Complete the following procedure to add a communication channel.

Step	Procedure
1.	Enter an appropriate <b>CC id</b> (only for V5.2).
2.	Select a row in the <b>Available Time Slots</b> list.
3.	Click on <b><i>Apply</i></b> to add a CC. If this is successful and a time slot is specified the new CC will be cross-connected to that time slot.
4.	Click on <b><i>Close</i></b> to exit the window.



### 5.4.6.3 Edit Communication Channel

This modal window is used to modify a CC id. It can be reached only via **Edit CC** from the *V5 Signalling* window (cf. Chapter 5.4.6, page 5-132).

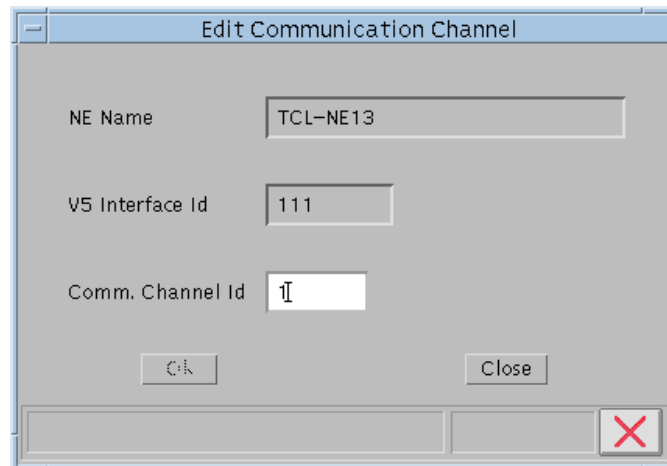


Figure 5-50 "Edit Communication Channel" Window

Parameters/ Buttons	Description
<b>Comm. Chan- nel id</b>	This field is used to enter the new value for the CC. This value is only taken into account for V5.2 Possible values: {0, 65503}.
<b>Ok</b>	This button is used to modify a CC to the given id. It is only enabled when a CC id is modified.

#### Procedure

Complete the following procedure to modify a communication channel.

Step	Procedure
1.	Enter a new <b>CC id</b> .
2.	Click on <b>Ok</b> to confirm.
3.	Click on <b>Close</b> to exit the window.

#### 5.4.6.4 Add Communication Path

This modal window is used to create a CP, while creating a CP it can be cross-connected to a CC (optional). It can be reached only via **Add CP** from the *V5 Signalling* window (cf. Chapter 5.4.6, page 5-132).

Figure 5-51 "Add Communication Path" Window.

Parameters/ Buttons	Description
<b>Comm. Path type</b>	<p>This option menu contains the possible types of CP.</p> <p>Possible values: PSTN, ISDN-Ds, ISDN-p, ISDN-f.</p> <p>Default: ISDN-Ds.</p> <p>⇒ <b>NOTE:</b>  <i>Control, Link control and BCC</i> communication paths are automatically created when a V5 Interface is created (cf. Chapter 5.4.1, page 5-83).</p>
<b>Comm. Path</b>	<p>This field is used to enter the identification number of the CP that shall be created.</p> <p>Possible values: {1, 9} for V5.1  {1, 145} for V5.2.</p>
<b>Comm. Channel id (optional)</b>	<p>This option menu contains the communication channels that are already created and the value None (default).</p> <p>Possible values: {0, 65503}.</p>
<b>Apply</b>	<p>This button is used to create a CP of the specified type with the given id. This button is enabled only when the identification number is specified.</p>

**Procedure**

Complete the following procedure to add a communication path.

<b>Step</b>	<b>Procedure</b>
1.	Use the option menu <b>Comm. Path type</b> to select an appropriate CP type.
2.	Enter the <b>CP id</b> .
3.	Use the option menu <b>Comm. Channel id</b> to select a CC id.
4.	Click on <b>Apply</b> to add a CP. If this is successful and a CC is specified the new CP is cross-connected to that CC, if there is not already a CP of that type cross-connected.
5.	Click on <b>Close</b> to exit the window.

### 5.4.6.5 Cross-Connect Communication Channel with Time Slot

This modal window is used to create a CC to time slot cross-connection. It can be reached only via **Add CC-TS** from the *V5 Signalling* window (cf. Chapter 5.4.6, page 5-132).

E1 Feeder	V5 Link Id	Timeslot
e1-1-1-3	7	15
e1-1-1-3	7	31
e1-1-4-1	9	16

Figure 5-52 "Crossconnect Communication Channel with Time Slot" Window

Parameters/ Buttons	Description
<b>Comm. Chan- nel id</b>	This option menu contains the list of all CCs that are not yet cross-connected to a timeslot.
<b>Available Time Slots</b>	<p><b>E1 Feeder:</b> Displays the physical feeder a timeslot belongs to.</p> <p><b>V5 Link id:</b> Displays the V5 Link id associated to the feeder shown in the previous field.</p> <p><b>Timeslot:</b> Displays the CC timeslots that are not in the protection mode and have no CC linked yet.</p> <p>Possible values: None, 15, 16, 31.</p>
<b>Apply</b>	This button is used to cross-connect the CC to the timeslot (if there is no other timeslot of the same type linked to that CC). This button is enabled only when both previous data have been specified.

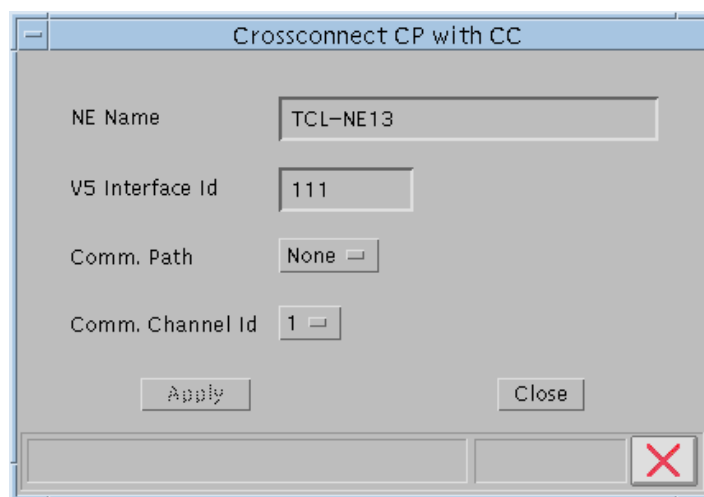
**Procedure**

Complete the following procedure to add a cross-connection between communication channel and time slot.

Step	Procedure
1.	Use the option menu <b>Comm. Channel id</b> to select an appropriate CC id.
2.	Select a row in the <b>Available Time Slots</b> list.
3.	Click on <b>Apply</b> to cross-connect the selected CC with the selected time slot.
4.	Click on <b>Close</b> to exit the window.

#### 5.4.6.6 Cross-Connect Communication Path with Communication Channel

This modal window is used to create a CP to CC cross-connection. It can be reached only via **Add CP-CC** from the *V5 Signalling* window (cf. Chapter 5.4.6, page 5-132).



**Figure 5-53 "Crossconnect CP with CC" Window**

Parameters/ Buttons	Description
<b>Comm. Path</b>	This option menu contains the list of all CPs that are not yet cross-connected to the CC.  Possible values: {1, 9} for V5.1 {1, 146} for V5.2.
<b>Comm. Channel Id</b>	This option menu contains all the CCs.  Possible values: {0, 65503}.
<b>Apply</b>	This button is used to cross-connect the CP to the CC, if there is no other CP of the same type linked to that CC.  This button is enabled only when both previous data have been specified.

**Procedure**

Complete the following procedure to add a cross-connection between communication path and communication.

Step	Procedure
1.	Use the option menu <b>Comm. Path</b> to select an appropriate CP.
2.	Use the option menu <b>Comm. Channel</b> to select an appropriate CC.
3.	Click on <b>Apply</b> to cross-connect the selected CP with the selected CC.
4.	Click on <b>Close</b> to exit the window.

### 5.4.6.7 V5.2 Group 2 Protection

#### Protection Groups

A protection group is used for defining a protection switching relationship where one or more standby timeslots provide protection for one or more working communication channels. The working (protected) channels and the standby (protecting) ones have to be provisioned. If a working timeslot, carrying a protected communication channel, becomes faulty a protection switch takes place. In this case a standby timeslot is selected for replacing the faulty one. If the faulty timeslot becomes operational again, it will be added to the protection group as an standby timeslot (non revertible switch). After recovering the V5.2 Interface, its initial provisioned configuration is re-established by the NE.

A V5.2 Interface supports two protection groups:

- Protection Group 1  
which can only have one working communication channel and only one standby timeslot associated. Protection Group 1 is automatically created if primary and secondary link are configured.
- Protection Group 2  
which can have up to 43 working communication channels protected and up to three standby timeslots. Protection Group 2 is automatically created if a protection or protection unit related to Group 2 is created.

Protection group 1 is handled via the *Primary Link* window (cf. Chapter 5.4.3, page 5-109) and *Secondary Link* window (cf. Chapter 5.4.4, page 5-111).

The following section describes the handling of protection group 2.

#### Window

The *V5.2 Group 2 Protection* window is used to create/show/remove displays the V5.2 group 2 protection structure of a V5 Interface. It shows the communication channel timeslots (TSs), the communication channels (CCs) current link and configured link. The main part is a table. Each row in the table presents a protection unit, with its timeslot.

This window can be reached only from *V5.2 Interface* window (cf. Chapter 5.4.1.2) via **Protection....**



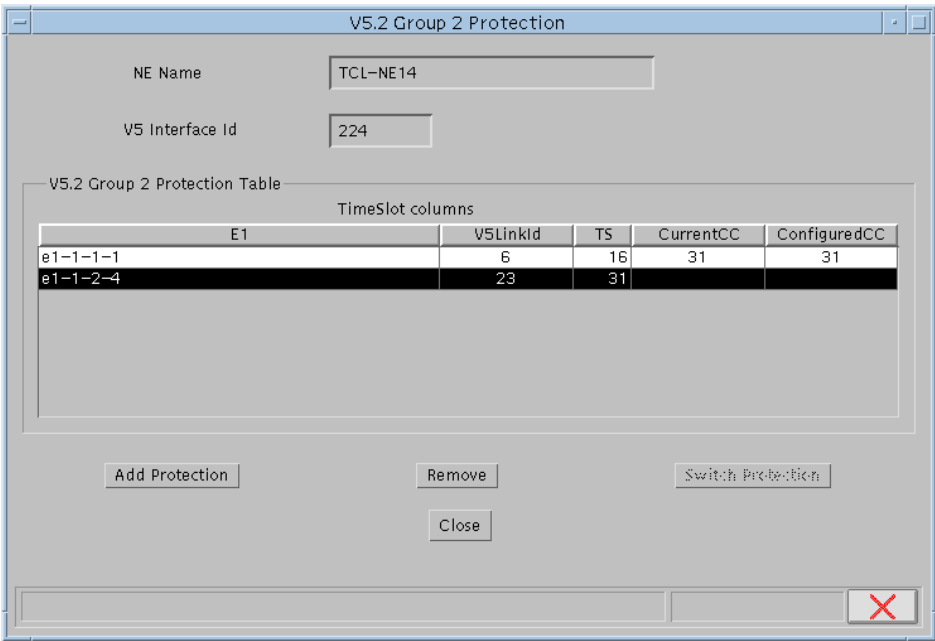


Figure 5-54 "V5.2 Group 2 Protection" Window

Parameters/ Buttons	Description
<b>V5. 2 Group 2 Protection Table</b>	<p>This table contains the V5.2 Group 2 Protection structure for the selected V5 Interface. Each line contains a timeslot, current CC and configured CC field. Each line can be selected separately.</p> <p>The operation that applies to a selected row is the remove operation (see below).</p> <p>No operations are possible as long as the administrative state of the V5 Interface is "Unlocked". Once it is "Locked" the current CC has no value, as it is not applicable. It only represents relevant data when the interface is running.</p> <p><b>E1 Feeder:</b> This column contains the physical feeder that carries the concerned timeslot.</p> <p><b>V5 Link id:</b> This column contains the V5 Link id of the link that is concerned.</p> <p><b>TS:</b> This column contains the timeslot number that corresponds to the concerned timeslot.</p> <p>Possible values: 15,16,31.</p> <p><b>Current CC:</b> This column identifies the communication channel via its CC id carried on this timeslot at this time. Only valid when the V5 Interface is "Unlocked".</p> <p><b>Configured CC:</b> This column defines the CC id of the communication channel that is carried on this timeslot on startup of the interface.</p>
<b>Command buttons</b>	<p><b>Add Protection:</b> This button provides access to the <i>Add V5.2 Group 2 Protection</i> window (modal - cf. Chapter 5.4.6.7.1).</p> <p>This button is only available when the V5 Interface is "Locked".</p> <p><b>Remove:</b> This button is only enabled when a row in the table is selected and the V5 Interface is "Locked".</p> <p>If the selected row contains a timeslot and a configured CC, the result is that the CC remains configured over that timeslot, but is no longer protected.</p> <p>If the selected row contains no configured CC, the timeslot is no longer available for protection.</p> <p><b>Switch Protection:</b> This button provides access to the <i>Switch V5.2 Group 2 Protection</i> window (modal - cf. Chapter 5.4.6.7.2).</p> <p>This button is only available when the V5 Interface is "Unlocked".</p>

<b>If you want to ...</b>	<b>then ...</b>
add a group 2 protection	click on <b>Add Protection</b> . The <i>Add V5.2 Group 2 Protection</i> window pops up (cf. Chapter 5.4.6.7.1).
to make a protection switch for a communication channel	click on <b>Switch Protection</b> . The <i>Switch V5.2 Group 2 Protection for CC</i> window pops up (cf. Chapter 5.4.6.7.2).
remove (delete) a already defined protection structure	select the desired row in the <b>V5. 2 Group 2 Protection Table</b> and click on <b>Remove</b> .
exit the window	click on the <b>Close</b> button.

#### 5.4.6.7.1 Add V5.2 Group 2 Protection

This modal window is used to add either a timeslot (protecting) or communication channel (protected) to the protection group 2 (i.e. to create a protection unit). It can be reached only from *V5.2 Group 2 Protection* window (cf. Chapter 5.4.6.7) via **Add Protection**.

E1 Feeder	V5 Link Id	Timeslot
e1-1-1-1	6	16
e1-1-2-4	23	31

**Figure 5-55 "Add V5.2 Group 2 Protection" Window**

Parameters/ Buttons	Description
<b>Comm. Channel id</b>	<p>This option menu contains the list of all CCs that are linked to a timeslot and not yet in the protection mode.</p> <p>When a value is selected, the corresponding timeslot is displayed in the timeslot field. The value "None" cannot be selected, but can be obtained when a timeslot is selected that has no CC linked.</p>
<b>Available Time Slots</b>	<p><b>E1 Feeder:</b> Displays the physical feeder a timeslot belongs to.</p> <p><b>V5 Link id:</b> Displays the V5 Link id associated to the feeder shown in the previous field.</p> <p><b>Timeslot:</b> Displays the CC timeslots that are not in the protection mode and have no CC linked yet.</p> <p>Possible values: None, 15, 16, 31.</p>

Parameters/ Buttons	Description
<b><i>Apply</i></b>	<p>This button is enabled when data have been selected in one of the above fields.</p> <p>In the case the selected value concerns a timeslot without CC, a protection unit is created for that timeslot that protects the other timeslots.</p> <p>If a timeslot is selected that carries a CC, a protection unit is defined for that timeslot and the CC is configured to it. That CC is then protected.</p>

**Procedure**

Complete the following procedure to add a group 2 protection.

Step	Procedure
1.	Select a row in the <b>Available Time Slots</b> list.
2.	Use the option menu <b>Comm. Channel id</b> to select an appropriate CC id.
3.	Click on <b><i>Apply</i></b> to create a group 2 protection.
4.	Click on <b><i>Close</i></b> to exit the window.

#### 5.4.6.7.2 Switch V5.2 Group 2 Protection

This modal window is used to switch timeslot/CC selection within the protection group 2. It can be reached only from *V5.2 Group 2 Protection* window (cf. Chapter 5.4.6.7) via **Switch Protection**.

E1 Feeder	V5 Link Id	Timeslot
e1-1-4-1	14	31
e1-1-4-2	15	15
e1-1-4-2	15	16

**Figure 5-56 "Switch V5.2 Group 2 Protection" Window**

Parameters/ Buttons	Description
<b>Protected Comm Channel Id</b>	This option menu contains the list of all CCs that are in the V5.2 group 2 protection mode.
<b>Protection timeslots</b>	<p>This option menu contains the timeslots that have no current CC and are in the protection group 2 of this V5.2 Interface.</p> <p><b>E1 Feeder:</b> Displays the physical feeder a timeslot belongs to.</p> <p><b>V5 Link id:</b> Displays the V5 Link id associated to the feeder shown in the previous field.</p> <p><b>Timeslot:</b> Displays the CC timeslots that are in the protection mode and have no CC linked yet.</p> <p>Possible values: None, 15, 16, 31.</p>

Parameters/ Buttons	Description
<b>Switch</b>	This button is enabled only when data have been selected in the above fields.  The V5.2 group 2 protection switch of the selected CC to the selected timeslot is executed.

**Procedure**

Complete the following procedure to execute a protection switch:

Step	Procedure
1.	Select a row in the <b>Protection timeslots</b> list.
2.	Use the option menu <b>Protected Comm Channel id</b> to select an appropriate CC id.
3.	Click on <b>Apply</b> . The protection switch is executed.
4.	Click on <b>Close</b> to exit the window.

#### 5.4.7 Move a V5 Interface in Service


**Procedure**

Complete the following procedure to move a V5 Interface in service:

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>Service -&gt; V5 Interface List</b> via the menu bar, select the desired <b>V5 Interface id</b> in the <i>V5 Interface List</i> window and click on <b>Edit V5 Interface....</b> The <i>V5 Interface</i> window pops up.
2.	Use the option menu <b>Administrative State</b> to change this parameter from "Locked" to "Unlocked".
3.	Click on <b>Apply</b> to confirm.
4.	Click on <b>Close</b> to exit the window.


### 5.4.8 Move a V5 Link in Service

**Procedure** Complete the following procedure to move a V5 Link in service:

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; E1 Feeders List</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Service -&gt; Provisioning -&gt; Edit/View</b> via the menu bar. The <i>E1 Feeder List</i> window pops up.
 <b>NOTE:</b> Do the following for all V5 links which should be moved in service.	
2.	Select a V5 link in the <b>E1 Feeders List</b> and click on <b>Edit V5 Link....</b> The <i>E1Feeder/V5 Link</i> window (tab V5 Link) pops up.
3.	Use the option menu <b>Administrative State</b> to change this parameter from "Locked" to "Unlocked".
4.	Click on <b>Apply</b> to confirm.
5.	Click on <b>Close</b> to exit the window.

### 5.4.9 Move a V5 User Port in Service

**Procedure** Complete the following procedure to move a V5 User Port in service:

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 User Port List</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Service -&gt; Provisioning -&gt; Edit</b> via the menu bar. The <i>V5 User Port List</i> window pops up.
 <b>NOTE:</b> Do the following for all V5 User Ports which should be moved in service.	
2.	Select a V5 User Port in the <b>V5 User Port List</b> and click on <b>Edit V5 User Port</b> . The <i>V5 PSTN User Port</i> window (or <i>V5 ISDN-BRA User Port</i> window) pops up.
3.	Use the option menu <b>Administrative State</b> to change this parameter from "Locked" to "Unlocked".



4. Click on **Apply** to confirm.
5. Click on **Close** to exit the window.

#### 5.4.10 Delete V5 User Port

**Procedure** Complete the following procedure to delete a V5 User Port.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 User Port List</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Service -&gt; V5 User Port List</b> via the menu bar. The <i>V5 User Port List</i> window pops up.
2.	Select an entry in the V5 User Port list and click on <b>Remove V5 User Port....</b> A <i>Warning</i> message pops up:  <div> <p><b>Removing V5 User Port may be service affecting. Do you want to continue?</b></p> <p>If you decide to continue, the AEM-NB will send a delete message to the NE:</p> <ul style="list-style-type: none"> <li>■ delete cross-connection between bearer channel and a V5 timeslot (for V5.1 protocol).</li> <li>■ delete cross-connection between V5 User Port and V5 Interface.</li> </ul> </div>

#### 5.4.11 Delete V5 Link

**Procedure** Complete the following procedure to delete a V5 Link.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; E1 Feeder List</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Service -&gt; Provisioning -&gt; Edit/View</b> via the menu bar. The <i>E1 Feeder List</i> window pops up.
2.	Select an entry in the <i>E1 Feeder List</i> and click on <b>Remove</b> . A <i>Warning</i> message pops up:  <div> <p><b>Removing V5 Link id may be service affecting. Do you want to continue?</b></p> <p>If you decide to continue, the AEM-NB will send a delete message to the NE:</p> </div>

- delete cross-connection between V5 communication channels and V5 protection group (V5.2).
- delete cross-connection between V5 communication channels and V5 timeslot (V5.2).
- delete cross-connection between V5 protection group and V5 Link's timeslots (V5.2).
- delete cross-connection between V5 Link and V5 Interface (V5.2).
- delete cross-connection between V5 communication channels and V5 Link's timeslots (V5.1).
- delete cross-connection between V5 User Port bearer channels and V5 Link's timeslots (V5.1).
- delete cross-connection between V5 communication path (control) and V5 communication channel (basic) (V5.1).
- delete V5 communication path (control), if provisioned (V5.1).
- delete V5 communication channel (basic), if provisioned and not cross-connected to any other V5 communication path (V5.1).
- delete cross-connection between V5 Link and V5 Interface (V5.1).

#### 5.4.12 Remove Communication Channel

**Procedure** Complete the following procedure to remove a communication channel.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>Service -&gt; V5 Interface List</b> via the menu bar, select the desired <b>V5 Interface id</b> in the <i>V5 Interface List</i> window and click on <b>Edit V5 Interface....</b> The <i>V5.x Interface</i> window pops up.
2.	Click on <b>Signalling....</b> The <i>V5 Signalling</i> window pops up
3.	Select an entry in the list and click on <b>Remove</b> . The AEM-NB will send a delete message to the NE: <ul style="list-style-type: none"> <li>■ delete cross-connection between V5 communication channel and a V5 timeslot.</li> <li>■ delete cross-connection between V5 communication path and V5 communication channel.</li> </ul>

### 5.4.13 Remove Communication Path

**Procedure** Complete the following procedure to remove a communication path.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>Service -&gt; V5 Interface List</b> via the menu bar, select the desired <b>V5 Interface id</b> in the <i>V5 Interface List</i> window and click on <b>Edit V5 Interface....</b> The <i>V5.x Interface</i> window pops up.
2.	Click on <b>Signalling....</b> The <i>V5 Signalling</i> window pops up
3.	Select an entry in the list and click on <b>Remove</b> . The AEM-NB will send a delete message to the NE: <ul style="list-style-type: none"> <li>■ delete cross-connection between V5 communication path and V5 communication channel.</li> </ul>

### 5.4.14 Remove Primary Link

A secondary link has to be removed (cf. Chapter 5.4.15, page 5-158) before a primary link can be removed.

**Procedure** Complete the following procedure to remove a primary link.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>Service -&gt; V5 Interface List</b> via the menu bar, select the desired <b>V5 Interface id</b> in the <i>V5 Interface List</i> window and click on <b>Edit V5 Interface....</b> The <i>V5.2 Interface</i> window pops up..
2.	Click on <b>Remove Primary</b> in the <b>Primary Link</b> field to remove the primary link.  After removing the primary link all automatically created entities are automatically removed: <ul style="list-style-type: none"> <li>■ cross-connection between V5 protection group 1 and V5 communication channel.</li> <li>■ cross-connection between V5 communication channel (basic) and V5 primary link's timeslot 16.</li> <li>■ cross-connection between V5 communication path (control) and V5 communication channel.</li> </ul>

- V5 communication path (control), if it is provisioned.
- cross-connection between V5 communication path (link control) and V5 communication channel.
- V5 communication path (link control), if it is provisioned.
- cross-connection between V5 communication path (BCC) and V5 communication channel.
- V5 communication path (BCC), if it is provisioned.
- cross-connection between V5 communication path and V5 communication channel (basic).
- cross-connection between V5 protection group 1 and a V5 Link's timeslot.
- V5 protection group 1, if it is provisioned.

#### 5.4.15 Remove Secondary Link

**Procedure** Complete the following procedure to remove a secondary link.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>Service -&gt; V5 Interface List</b> via the menu bar, select the desired <b>V5 Interface id</b> in the <i>V5 Interface List</i> window and click on <b>Edit V5 Interface....</b> The <i>V5.2 Interface</i> window pops up.
2.	Click on <b>Remove Secondary</b> in the <b>Secondary Link</b> field to remove the secondary link.
	After removing the secondary link all automatically created entities are automatically removed.

#### 5.4.16 Remove V5 Protection Group 2

**Procedure** Complete the following procedure to remove a V5 protection group 2.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 Interface List -&gt; V5 Interface id</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>Service -&gt; V5 Interface List</b> via the menu bar, select the desired <b>V5 Interface id</b> in the <i>V5 Interface List</i> window and click on <b>Edit V5 Interface....</b> The <i>V5.2 Interface</i> window pops up.
2.	Click on <b>Protection....</b> The <i>V5.2 Group 2 Protection</i> window pops up.

3. Select an entry in the table and click on **Remove**. The AEM-NB will send a delete message to the NE:
  - delete cross-connection between V5 protection group 2 and V5 communication channel.
  - delete cross-connection between V5 protection group 2 and V5 timeslot.
  - delete cross-connection between V5 protection group 2 and V5 communication channel or V5 timeslot.

**NOTE:**

If all protecting and protected units are deleted the protection group is also deleted.

### 5.4.17 Delete V5 Interface

To be able to delete a V5 Interface it is necessary previously to delete the following:

- remove V5 protection group 2, if it is configured (cf. Chapter 5.4.16, page 5-158).
- remove secondary link, if it is configured (cf. Chapter 5.4.15, page 5-158).
- remove primary link, if it is configured (cf. Chapter 5.4.14, page 5-157).
- delete all V5 communication paths contained in the V5 Interface (cf. Chapter 5.4.13, page 5-157).
- delete all V5 communication channel contained in the V5 Interface (cf. Chapter 5.4.12, page 5-156).
- delete all cross-connection between V5 User Ports and V5 Interface (cf. Chapter 5.4.10, page 5-155).
- delete all cross-connections between V5 Links and V5 Interface (cf. Chapter 5.4.11, page 5-155).

**Procedure**

Complete the following procedure to delete a V5 Interface.

Step	Procedure
1.	Select <b>All -&gt; NE -&gt; V5 Interface List</b> in the Network Browser and <b>Edit</b> via the cursor menu or select <b>File -&gt; Open</b> or <b>Service -&gt; Provisioning -&gt; Edit</b> or <b>Service -&gt; V5 Interface List</b> via the menu bar. The <i>V5 Interfaces List</i> window pops up.
2.	Select a V5 Interface id and click on <b>Remove</b> . The AEM-NB will send a delete message to the NE.



---

## Contents

<b>6.1</b>	<b>Overview</b>	<a href="#"><u>6-1</u></a>
<b>6.2</b>	<b>Alarm Management</b>	<a href="#"><u>6-1</u></a>
6.2.1	Overview	<a href="#"><u>6-1</u></a>
6.2.2	Maintain Up-To-Date Alarm Information	<a href="#"><u>6-2</u></a>
6.2.3	Alarm Notification to the User	<a href="#"><u>6-3</u></a>
6.2.4	Provide Access to the Current Alarm Data	<a href="#"><u>6-7</u></a>
6.2.5	Managing the Raising of Alarms	<a href="#"><u>6-7</u></a>
6.2.6	Manage Alarm Acknowledgment	<a href="#"><u>6-8</u></a>
6.2.7	Managing the Clearing of Alarms	<a href="#"><u>6-8</u></a>
6.2.8	Alarm Data Synchronization	<a href="#"><u>6-8</u></a>
6.2.9	AEM-NB Alarm Log Handling	<a href="#"><u>6-9</u></a>
6.2.10	Periodical Deletion of Cleared Alarms	<a href="#"><u>6-9</u></a>
<b>6.3</b>	<b>Alarm Monitoring</b>	<a href="#"><u>6-10</u></a>
6.3.1	General	<a href="#"><u>6-10</u></a>
6.3.2	Starting and Terminating the Alarm Viewer	<a href="#"><u>6-10</u></a>
6.3.2.1	Starting the Alarm Viewer	<a href="#"><u>6-10</u></a>
6.3.2.2	Terminating the Alarm Viewer	<a href="#"><u>6-11</u></a>
6.3.3	Performing Alarm Viewer Functions	<a href="#"><u>6-11</u></a>
6.3.3.1	Menu Bar	<a href="#"><u>6-12</u></a>
6.3.3.2	Toolbar	<a href="#"><u>6-14</u></a>
6.3.3.3	General Information Section	<a href="#"><u>6-14</u></a>
6.3.3.4	Alarm Table	<a href="#"><u>6-15</u></a>
6.3.3.4.1	Alarm Parameters	<a href="#"><u>6-15</u></a>
6.3.3.4.2	Sorting Alarms	<a href="#"><u>6-17</u></a>
6.3.4	System Management Functions	<a href="#"><u>6-18</u></a>
6.3.4.1	File	<a href="#"><u>6-18</u></a>
6.3.4.2	Views	<a href="#"><u>6-18</u></a>

---

# Contents

6.3.4.3	Filters	<a href="#">6-19</a>
6.3.4.4	Help	<a href="#">6-21</a>
6.3.5	Alarm Viewer Functions	<a href="#">6-21</a>
<b>6.4</b>	<b>Test Management</b>	<a href="#">6-23</a>
6.4.1	User Line Test	<a href="#">6-25</a>
6.4.2	User Port Test	<a href="#">6-29</a>
6.4.3	Standby Card Test Scheduling	<a href="#">6-31</a>
6.4.4	Built-in Self-Test	<a href="#">6-32</a>
6.4.5	TAP-Test	<a href="#">6-33</a>
6.4.6	CRC Test	<a href="#">6-34</a>
6.4.7	Loopback Test at the Feeder Side	<a href="#">6-37</a>
6.4.8	Loopback Test at the ISDN User Port Side	<a href="#">6-38</a>
<b>6.5</b>	<b>Information Management and Maintenance</b>	<a href="#">6-40</a>
6.5.1	NE-AEM-NB Connection States	<a href="#">6-40</a>
6.5.2	Changing Connection States	<a href="#">6-40</a>
6.5.3	Configuration Data Synchronization after Association	<a href="#">6-41</a>
6.5.4	Alarm Data Synchronization after Association	<a href="#">6-42</a>
6.5.5	Association Maintenance	<a href="#">6-43</a>
<b>6.6</b>	<b>Alarms</b>	<a href="#">6-44</a>
6.6.1	Overview	<a href="#">6-44</a>
6.6.2	Alarm Types	<a href="#">6-44</a>
6.6.3	Network Element Alarms	<a href="#">6-46</a>
6.6.4	Element Manager Platform Alarms	<a href="#">6-46</a>
6.6.4.1	LOG_DEL_FULL	<a href="#">6-46</a>
6.6.4.2	LOG_DEL_PART	<a href="#">6-47</a>
6.6.4.3	NEASSOC_FAILED	<a href="#">6-47</a>
6.6.4.4	NEASSOC_LOST	<a href="#">6-48</a>
6.6.4.5	SWVR_ILLEGAL	<a href="#">6-49</a>
6.6.4.6	TCP/IP_CON_REFUSED	<a href="#">6-49</a>
6.6.4.7	TL1_COMM_DENIED	<a href="#">6-50</a>



## 6.1 Overview

---

This chapter provides you with informations about

- Basics on the alarm management
- Basics on alarms
- Maintenance actions if certain alarms are pending
- Using the Alarm Viewer
- Performing test actions with the test management
- Basics on information management (e.g. connection states).

## 6.2 Alarm Management

---

### 6.2.1 Overview

---

The main function of the alarm management is to manage the *AnyMedia*® Access System Element Manager for Narrowband Services (AEM-NB) and Network Element (NE) related alarms that are registered in the Element Manager System (EMS). For the list of the NE alarms refer to Chapter 6.6.3, page 6-46. For the list of the alarms generated by the management system refer to Chapter 6.6.4, page 6-46.

Once the communication connection between the AEM-NB and an NE is established, the AEM-NB clears the "not-connected" NE alarm indication (if they exist) and starts an alarms and environment alarms synchronization process between the AEM-NB alarm database and active NE alarms. Finally the AEM-NB will try to update its view of NE configuration data and will start a synchronization process between the AEM-NB data set and the NE configuration information (NE NVDS). The NE database is always the master.

The database does not maintain the alarm history, it only stores the current alarms status. An alarm can be in one of the following three states:

- Raised
- Acknowledged
- Cleared.

The main responsibilities of the Alarm Management Subsystem (AMS) are the following:

- Maintain up-to-date alarm information.
- Notify alarm changes to alarm clients.
- Provide access to the current alarm data.
- Manage alarms raising.
- Manage cleared alarms.
- Manage acknowledgment of alarms.
- Synchronization of the alarm data per NE.
- AEM-NB Alarm log handling.
- Periodical deletion of cleared alarms.

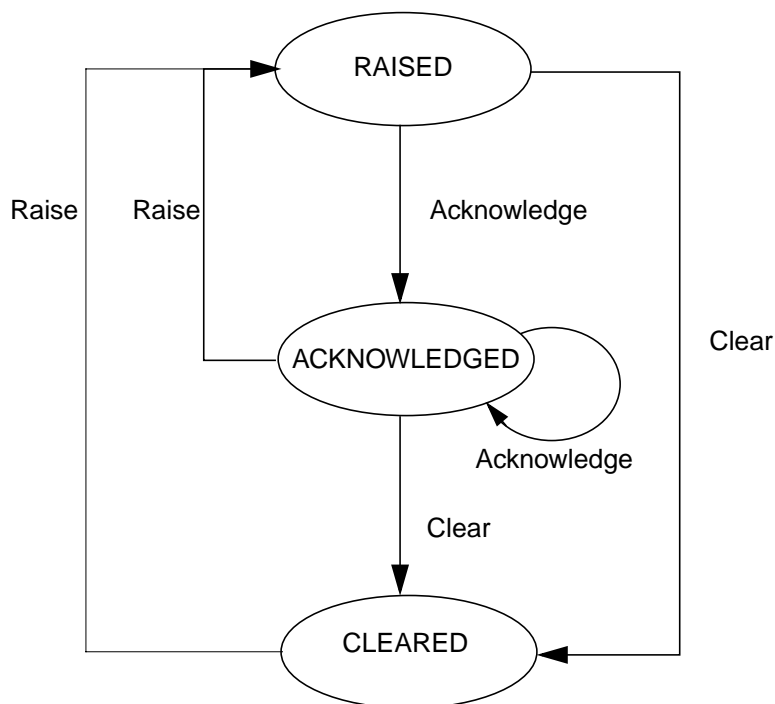
#### 6.2.2 Maintain Up-To-Date Alarm Information

---

During the alarm life time, the AEM-NB updates the following information:

- The date and time of the last status change.
- The last alarm status change.
- The last user (id) which acknowledged an alarm.
- The number of times the alarm has occurred between the first occurrence and now.

If an acknowledged alarm is raised again the status for this alarm is changed from acknowledged to raised. Additionally the acknowledge data (*user Id*), if available, is removed from the alarm information.



**Figure 6-1 Life Cycle of an Alarm**

### 6.2.3 Alarm Notification to the User

#### Overview

Any time incorrect data (out-of-range values, inappropriate value types, etc.) is entered at the Graphical User Interface (GUI), a new alarm occurs or the status of any alarm changes to raised again, an alarm message is reported to the AEM-NB. The alarms are indicated, if defined, visually and acoustically.

#### Visual Alarm Indication

The occurrence of a new alarm of a defined severity (default value: critical) is visually indicated in different ways:

- Notification icon displayed in the AEM-NB access bar.

This icon consists of a flag and a counter. The flag is raised only the first time a new alarm of the defined severity is reported to the AEM-NB. Additionally the counter is increased.

Every time the user clicks on the icon, the flag is lowered and the counter is reset before the AEM-NB requires confirmation.

The alarm severity affecting the notification icon is configurable via the system variables in the file \$ANYMEDIAPATH/GUI/cfg/SystemPreferences.ini.

**Table 6-1 Configure Notification Icon**

System Variable	Severity	Possible States
VISUAL_CRITICAL_ALARM_SEV	Critical	On/Off, default = ON
VISUAL_MAJOR_ALARM_SEV	Major	On/Off, default = OFF
VISUAL_MINOR_ALARM_SEV	Minor	On/Off, default = OFF
VISUAL_INFO_ALARM_SEV	Information	On/Off, default = OFF

For alarm notification see also Chapter 3.2.3.1.

■ Shelf View Window

This window (cf. Figure 6-2, page 6-6) provides general inventory, provisioning and alarm information (through the plug-in LEDs). Each slot shows the card type inserted and its alarms (via a red FLT LED, if available). If the slot is empty, no card will be shown.

See table below for the list of LEDs provided in each plug-in. The table describes the colors used when the LED is ON or blinking. If the LED is OFF the color black is used.

**Table 6-2 LED Meanings**

Circuit Pack	LED	Color	Meanings
IO_E1	FLT	red	<ul style="list-style-type: none"> <li>■ Lit during plug-in failure.</li> <li>■ Flashes when the plug-in executes off-line self-test.</li> </ul>
	ACT	green	Lit when the plug-in is service-active.
	CLF1	yellow	Lit when a fault or facility alarm occurs on the in service received E1 port 1.
	CLF2	yellow	Lit when a fault or facility alarm occurs on the in service received E1 port 2.
	CLF3	yellow	Lit when a fault or facility alarm occurs on the in service received E1 port 3.
	CLF4	yellow	Lit when a fault or facility alarm occurs on the in service received E1 port 4.

**Table 6-2 LED Meanings**

<b>Circuit Pack</b>	<b>LED</b>	<b>Color</b>	<b>Meanings</b>
COMDAC	FLT	red	<ul style="list-style-type: none"> <li>■ Lit when a fault is detected on the plug-in.</li> <li>■ Flashes during software download and turnup.</li> </ul>
	ACT	green	Indicates that this COMDAC is active.
	CR	red	Lit when the highest severity alarm is critical.
	MJ	red	Lit when the highest severity alarm is major.
	MN	yellow	Lit when the highest severity alarm is minor.
	NE	yellow	Lit when the source of the fault or abnormal condition is near end.
	FE	yellow	Lit when the source of the fault or abnormal condition is far end.
CIU	FLT	red	Lit when a fault is detected on the plug-in.
	ACT	green	Lit when a test is in progress. Plug-in id in operation.
	POW1	green	Lit when -48V. Power supply A is in operation.
	POW2	green	Lit when -48V. Power supply B is in operation.
	TC	green	Lit when test is in progress (TAP100 connected).
	MISC	yellow	Lit when one of the eight miscellaneous alarm inputs is active.
	ACO	green	Alarm Cut-off reminder
Application Packs	FLT	red	<ul style="list-style-type: none"> <li>■ Lit when a fault is detected on the AP</li> <li>■ Flashes when the plug-in executes off-line shelf-tests.</li> </ul>
IO_HDLC	FLT	red	<ul style="list-style-type: none"> <li>■ Lit when a fault is detected on the plug-in</li> <li>■ Flashes when the plug-in executes off-line shelf-test.</li> </ul>
	ACT	green	Lit when the plug-in is service-active.

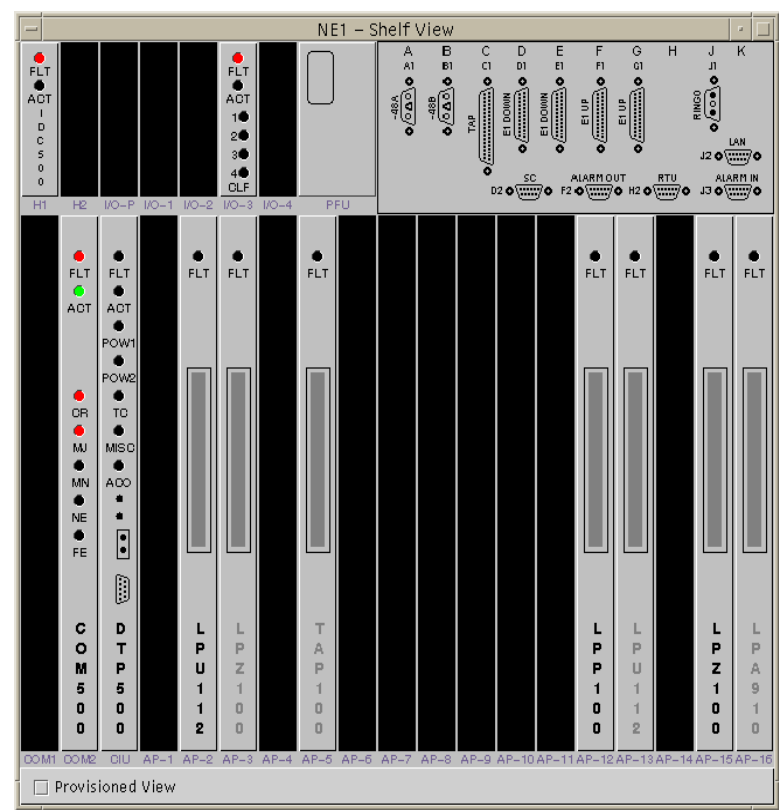


Figure 6-2 Shelf View

**Audible Indication**

The user is warned by an audible indication if a new alarm of a defined severity (default value: critical) is reported to the AEM-NB. Only alarms from NEs within the user domain will be indicated. Alarms are audible on the server only.

The alarm severity which causes audible alarm notification is configurable via the system variables in the file \$ANYMEDIAPATH/GUI/cfg/SystemPreferences.ini.

Table 6-3 Configure Audible Notification

System Variable	Severity	Possible States
AUDI_CRITICAL_ALARM_SEV	Critical	On/Off, default = ON
AUDI_MAJOR_ALARM_SEV	Major	On/Off, default = OFF
AUDI_MINOR_ALARM_SEV	Minor	On/Off, default = OFF
AUDI_INFO_ALARM_SEV	Information	On/Off, default = OFF

For alarm notification see also Chapter 3.2.3.1.

By default, the AEM-NB causes an audible alarm indication every time a new critical alarm is reported to the AEM-NB.

<b>Alarm Information</b>	For more information on the reported alarm open the Alarm Viewer (cf. Chapter 6.3, page 6-10).
<b>Alarm Acknowledgment</b>	Acknowledging alarms is described in Chapter 6.3.5, page 6-21.
<b>Alarm Clearance</b>	Clearing alarms is described in Chapter 6.3.5, page 6-21.

#### 6.2.4 Provide Access to the Current Alarm Data

<b>Alarm Retrieval</b>	<p>The user can select lists of alarms filtered by several fields. Therefore the user specifies a selection criterion (cf. Chapter 6.3.4.3, page 6-19) that is taken by the AMS to make the appropriate filters. For instance, an user can request all the critical alarms of an NE, or all platform alarms, or all alarms which are service affecting and are raised at the same time.</p> <p>The number of alarms stored in the alarm database can be retrieved, too. The total number of alarms can be retrieved as well as the number of alarms per severity (number of critical alarms, major, minor and information).</p>
<b>User Domains</b>	<p>The user domain is the list of NEs and/or the AEM-NB the user can manage. The user domains are applicable in the AMS to the alarm retrieval operations and to the alarm notification.</p> <p>Each user can only request alarms and the number of alarms that are in the user's domain. The client and server security filters fill in this information. When the alarm retrieval operation arrives at the alarm server, in addition to the normal input data it also contains the user domain information added by the user interface.</p>

#### 6.2.5 Managing the Raising of Alarms

<b>General</b>	An alarm is raised by the NE or by any object of the AEM-NB. When an alarm is raised its state and the relevant transmitted data (cf. Chapter 6.6.2, page 6-44) are updated. Special care has to be taken if the alarm is raised repeatedly (see "Repetitive and Fluctuating Alarms"). In this case the already existing alarm is put into the raised state. The user acknowledge identification, if available, is removed from the alarm. This way a raised condition of an existing alarm is considered as a new raising (not a new alarm). The number of occurrences is increased every time the same alarm is raised.
<b>Repetitive and Fluctuating Alarms</b>	A repetitive alarm is an alarm that is raised several times before it is cleared. A fluctuating alarm is an alarm that is raised and cleared alternatively several times in a short period (at least less than the AEM-NB constant for the cleared alarms, see Chapter 6.2.10, page 6-9).

To handle these alarms three fields are defined and maintained for each alarm:

- First Raised Time
- Last Changed Time
- Number of Occurrences.

The alarm viewer can obtain the following information:

- The "Number of Occurrences" is the number of times the alarm has been raised between when it was first raised and the current time (only the raised alarms are counted). In this period the alarm has been raised all the time or it may have been raised/cleared several times (it is not relevant to distinguish both cases).

### **6.2.6 Manage Alarm Acknowledgment**

---

Alarms can only be acknowledged by a user at the user interface. It is possible to acknowledge all alarms types. If an alarm is acknowledged its state is updated accordingly and the user identification and the last changed time are registered. Acknowledging an alarm causes a change to the alarm database. Therefore the alarm was logged before in the action log. It is possible to acknowledge an alarm that has already been acknowledged. The user identification and the new acknowledge time are registered as well, overwriting the previous acknowledge data.

### **6.2.7 Managing the Clearing of Alarms**

---

#### **General**

The NE alarms are cleared by the NE-AMS. Platform alarms are cleared automatically (e.g. NE-AEM-NB association alarms) or by a user at the user interface (e.g. log alarms). Users can only clear specific platform alarms. Users cannot clear the association alarms for the NE alarms. When an alarm is cleared its state is updated and the time is registered, too. Clearing an alarm causes a change to the alarm database. Therefore the alarm was logged before in the autonomous report log (if the user clears an alarm this will be logged in the action log; if an alarm is cleared by the NE it will be logged in the autonomous report log).

If the raise is newer, then it is a repetitive raise; the alarm state is set to the raised state. If the raise is older, then this message is ignored; the alarm state stays in the cleared state and the relevant data is updated.

### **6.2.8 Alarm Data Synchronization**

---

The AMS is responsible for the performance of NE alarm synchronization. To accomplish this, the AMS requests all the current alarms (normal and environment) of the NE that is being synchronized. Once the AMS has received these alarms it compares them with the alarms stored in the AEM-NB alarm database. At the end of the synchronization the alarms stored in the alarm database must be the same as the alarms retrieved from the NE-AMS. Only one synchronization per NE can be performed at the same time. The AMS rejects any synchronization request for the same NE if the first one has still not finished.



### 6.2.9 AEM-NB Alarm Log Handling

If the user wants to know the different states throughout the alarm life the user will have to see the Log System (cf. Chapter 3.7, page 3-31) in which all alarm changes are stored.

Three types of logs are used. The AMS logs the following situations:

- Actions log:
  - Periodical database deletion of cleared alarm's start and end.
  - Alarm's synchronization start and end.
  - Periodical deletion of cleared alarms.
  - Manual clear, manual acknowledge. The user identification that performs these actions is also logged.
- System-internal events log:
  - Exception conditions of the AMS.
- Autonomous report log:
  - Raise, automatic clear, update of every alarm.

### 6.2.10 Periodical Deletion of Cleared Alarms

By default, alarms with *cleared* status are maintained for at least three days (including the current day) in the database. This value can be configured by the user via the system variable "AM.minimumClearPeriod" in the file \$ANYMEDIAPATH/cfg/AnyMediaNBEM.cfg and is an integer multiple in days. The default value is 3 days.

The AEM-NB performs a periodical deletion of the alarms with cleared status that exceed the specified time. This is done during the night period in low-load hours.

---

## 6.3 Alarm Monitoring

---

### 6.3.1 General

---

#### Overview

The AEM-NB provides a process to monitor and display all alarms stored in the database. Using this system, the Alarm Viewer, the user is able to see many different alarm attributes such as Alarm Type, Severity, Status, Summary and the date and time when the alarm was raised. Via this tool the user can perform actions (e.g. acknowledge, clear) for some of these alarms.

#### What you will find

In this chapter you will find the following information:

- Instructions for starting and terminating the alarm viewer (Chapter 6.3.2, page 6-10)
- Instructions for handling the alarm viewer (Chapter 6.3.3, page 6-11)
- Structure of the alarm viewer window (Chapter 6.3.3.3, page 6-14 and Chapter 6.3.3.4, page 6-15)
- System management (Chapter 6.3.4, page 6-18)
- Alarm viewer functions (Chapter 6.3.5, page 6-21).

### 6.3.2 Starting and Terminating the Alarm Viewer

---

#### 6.3.2.1 Starting the Alarm Viewer

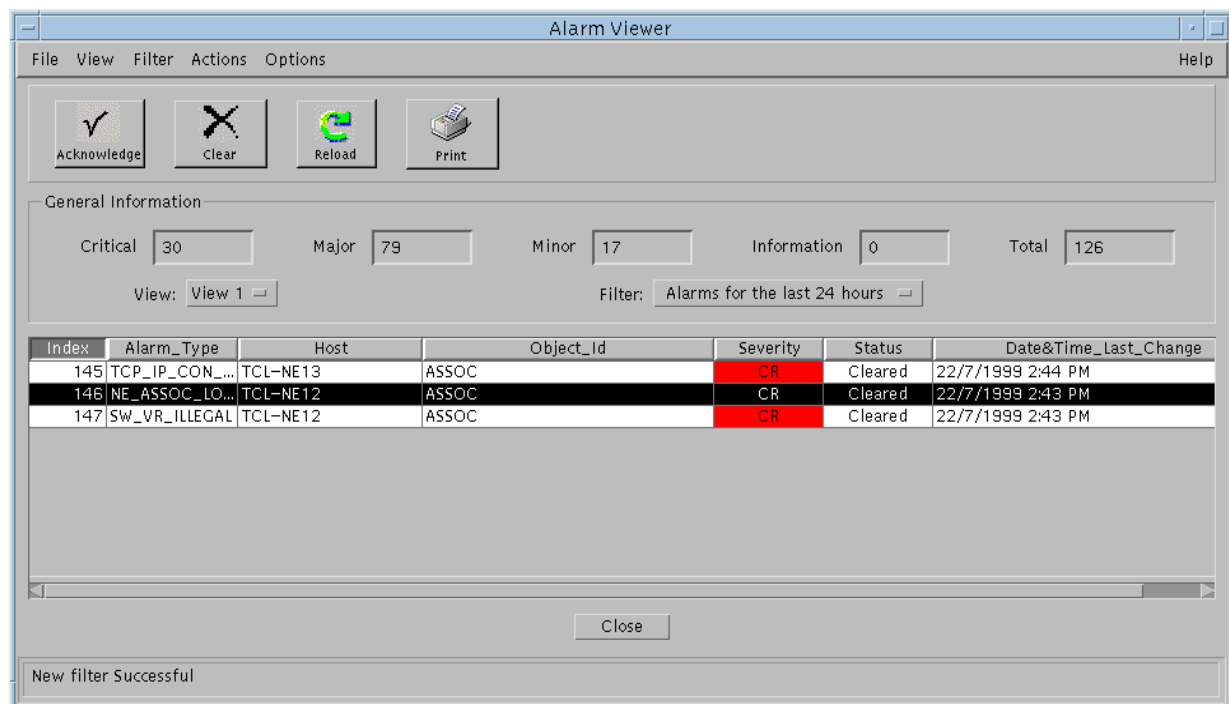
The Alarm Viewer can be started in different ways:

- Clicking on the icon **Alarm Viewer** in the Access Bar (cf. Chapter 3.2.3, page 3-4).
- Clicking on **Alarms** in the menu bar of the other Element Manager applications (cf. Chapter 3.3.6, page 3-11). In this case only alarms of the NE which is selected in the Network Browser are shown.
- Selecting **File -> New** in the Alarm Viewer.

The displayed window has the title "Alarm Viewer" and maintains similarities with the other AEM-NB's windows.

The *Alarm Viewer* window consists of the sections:

- Menu bar (File, Views, Filters, Actions, Help).
- Toolbar (buttons for Acknowledge, Clear, Reload and Print).
- General Information section.
- Alarm table.



**Figure 6-3 Alarm Viewer Window**

### 6.3.2.2 Terminating the Alarm Viewer

The Alarm Viewer can be terminated as follows:

- By selecting **File -> Exit** in the Alarm Viewer menu to close all Alarm Viewers launched by the user.
- By clicking on **Close** button or **File -> Close** to close only the Alarm Viewer being in use.

Before quitting the Alarm Viewer the user is prompted for confirmation.

### 6.3.3 Performing Alarm Viewer Functions

The Alarm Viewer provides different possibilities to perform internal functions and alarm management functions.

These functions can be initiated via:

- Menu
- Toolbar

In most cases the choice depends on the user's personal preference.

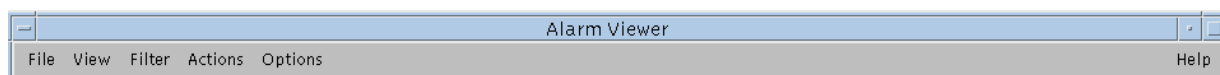
### 6.3.3.1 Menu Bar

The menu is used to activate alarm viewer functions.



**NOTE:**

The executable functions depend on your user privileges.



**Figure 6-4 Menu Bar of the Alarm Viewer**

Selection is achieved

- By opening the menu by pressing the left mouse button and dragging the cursor to the desired option in the menu or
- By opening the menu via the keyboard by entering **Alt** plus the underlined letter of the relevant menu to open the menu option and then entering the letter underlined in the desired menu option.

**Table 6-4 File Menu**

Menu display	Menu option	Meaning	Information in
	New	Launch a new instance of the Alarm Viewer.	Chapter 6.3.4.1, page 6-18
	Print -> Print Table	Print all alarm items displayed in the currently displayed table or save the items into an ASCII file. The Print Dialog window (cf. Chapter 3.5) is opened.	
	Print -> Preview	Shows the "Print Preview" window (cf. Chapter 3.5) .	
	Print -> Print Window	Prints a screenshot of the whole window. The Print Dialog is opened (cf. Chapter 3.5).	
	Close	Dismiss this window, but without closing other instances of the Alarm Viewer.	
	Exit	Close all Alarm Viewers opened by the user.	

**Table 6-5 Views Menu**

Menu display	Menu option	Meaning	Information in
<div>View1 View2 View3 View 4</div>	View1	Select a view from the predefined views.	Chapter 6.3.4.2, page 6-18
	View2		
	View3		
	View4		

**Table 6-6 Filters Menu**

Menu display	Menu option	Meaning	Information in
<div>Alarms for the last 24 hours Critical Raised Alarms Raised Alarms Alarms from a Host/s Critical Alarms not cleared Owned Acknowledge Alarms Clear Alarms All Acknowledge Alarms None Filter / All Alarms</div>	Alarms for the last 24 hours	Selection of filter criteria for displaying alarm information.	Chapter 6.3.4.3, page 6-19
	Critical Raised Alarms		
	Raised Alarms		
	Alarms from a Host/s		
	Critical Alarms not cleared		
	Owned Acknowledge Alarms		
	Clear Alarms		
	All Acknowledge Alarms		
	None Filter / All Alarms		

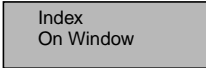
**Table 6-7 Actions Menu**

Menu display	Menu option	Meaning	Information in
<div>Acknowledge Clear Reload</div>	Acknowledge	Acknowledge all selected alarms, their status will change to acknowledged.	Chapter 6.3.5, page 6-21
	Clear	Clear all selected alarms, their status will change to cleared.	
	Reload	Display a fresh copy of the current information shown in the window. Only alarms which match the filter criteria will be included.	

**Table 6-8 Options Menu**

Menu display	Menu option	Meaning	Information in
<div>Automatic Reload</div>	Automatic Reload	If this option is checked the Alarm Viewer is automatically updated every minute. If it is not checked the update has to be manually done via <b>File -&gt; Reload</b> .	Chapter 6.3.5, page 6-21





**Table 6-9 Help Menu**

Menu display	Menu option	Meaning	Information in
	Index	Display the index help, allowing the user to navigate through the AEM-NB help information.	Chapter 6.3.4.4, page 6-21
	On Window	Display the help information of the window where the user is currently working.	

### 6.3.3.2 Toolbar

The toolbar contains often used functions and consists of four buttons:

**Table 6-10 Toolbar**

Function	Icon	Meaning
Acknowledge		Acknowledge all selected alarms. Their status immediately changes to acknowledged. The User_Ack is set to the login of the user who has acknowledged the alarm
Clear		Clear all selected alarms. Their status immediately changes to cleared.
Reload		Reload the actual alarms states into the table. Only alarms which match the filter criteria are included.
Print		Opens a submenu (Print Table, Print Window, Print Preview) than one of these items can be selected..

### 6.3.3.3 General Information Section

The first section is a frame titled *General Information*, this frame includes controls showing information about the number of alarms of each alarm severity (in the domain where the user is working):

- Critical  
Displays the number of critical (CR) alarms.
- Major  
Displays the number of major (MJ) alarms.
- Minor  
Displays the number of minor (MN) alarms.

- Information  
Displays the number of information (IN) alarms.
- Total  
Displays the total number of alarms (all severities).

Additionally the frame contains two option menus, which show the filter (cf. Chapter 6.3.4.3, page 6-19) and view (cf. Chapter 6.3.4.2, page 6-18) currently being used. In this two option menus the user can select filters and views.

**Figure 6-5** Frame General Information

### 6.3.3.4 Alarm Table

The last section in the Alarm Viewer window is a table that contains zero or more alarms belonging to a domain. This table allows the user to sort the alarms (cf. Chapter 6.3.3.4.2, page 6-17) by clicking on a specific table header. The user also can select them for acknowledgment or clearance. The mechanism to acknowledge or clear is the same, the user has to select one or more alarms. After selecting the alarms click on **Acknowledge** or **Clear** in the tool bar or select **Actions -> Acknowledge** or **Actions -> Clear** via the menu bar.

Index	Alarm_Type	Host	Object_Id	Severity	Status	Date&Time_Last
14	NE_ASSOC_LO...	NE3	ASSOC	CR	Cleared	26/1/1999 10:47 AM
28	LOG_DEL_FULL	AnyMedia	Ac_TASK	MJ	Raised	26/1/1999 10:56 AM
32	LOG_DEL_FULL	AnyMedia	Act_TASK	MJ	Raised	26/1/1999 9:20 AM
33	LOG_DEL_FULL	AnyMedia	lee_TASK	MJ	Raised	26/1/1999 8:56 AM
35	SW_VR_ILLEGAL	NE3	ASSOC	CR	Cleared	26/1/1999 10:47 AM
36	TL1_COMM_D...	NE3	ASSOC	CR	Cleared	26/1/1999 10:47 AM
37	LOG_DEL_PART	AnyMedia	lee_TASK	MN	Raised	25/1/1999 11:56 PM
38	LOG_DEL_PART	AnyMedia	Ac_TASK	MN	Raised	26/1/1999 3:41 AM
39	LOG_DEL_PART	AnyMedia	Act_TASK	MN	Raised	26/1/1999 4:26 AM

**Figure 6-6** Alarm List Section

#### 6.3.3.4.1 Alarm Parameters

For each alarm the following alarm fields (depending on the selected view) can be displayed:

- Index  
Sequence number for each different alarm reported to the AEM-NB (the maximum sequence number is 100 000).

- **Alarm\_Type**  
Unique identification of each alarm type.
- **Summary**  
Contains text briefly describing the alarm. The summary text is unique in the Element Manager.
- **Severity**  
Contains the default severity of the alarm.
  - Critical (*CR*)
  - Major (*MJ*)
  - Minor (*MN*)
  - Information (*IN*)
- **Service Affecting**  
Specifies whether the alarm is subscriber service affecting or not.  
Possible values: Yes, No.
- **Description**  
Contains a full description of the alarm.
- **Host**  
Unique text label in the AEM-NB scope. For NE alarms, it is the "NE-Name" that identifies the NE through all the AEM-NB applications the alarm belongs to. For platform alarms, it is the string "EM".
- **Object\_Id**  
Object identifier referring to the alarm. Examples of objects are network elements, "ap-1-1", etc.
- **Status**  
Working status of the alarms.
  - Raised  
Alarm with alarm condition raised, and has not been yet processed.
  - Acknowledged  
The alarm is still active and being investigated.
  - Cleared  
Alarm condition has been cleared, or the user has requested the clearing of this alarm.
- **Date&Time First Raise**  
Date and Time of the first Raised status in the life cycle of one alarm.
- **Date&Time Last Change**  
Date and Time of the last status change in the life cycle of one alarm.



- Occurrences

Number of times the alarm has been raised between the first raised time and the current time.

- User Ack

The login of the last user which has acknowledged an alarm.

#### 6.3.3.4.2 Sorting Alarms

##### Summary

The user can sort alarms by the different fields by clicking on the respective header. The sort can be ascending or descending order. The sort order is reversed by clicking on the respective header.

All alarm fields are sorted by alphanumeric order except dates, severity and status fields.

- In the severity field, alarms are sorted in the logical order: Critical, Major, Minor and Information.
- In the status field, alarms are sorted in the logical order: Raised, Acknowledge and Clear.

##### Effects

The alarms are re-arranged according to the selected criteria.

##### Sorting Alarms

Proceed as follows to sort the alarm display:

Step	Procedure
1.	Click on the header according to which the alarms are to be sorted.
	<i>Response:</i> The alarms are sorted according to the selected alarm field in ascending or descending order.
2.	Check if the list was sorted as desired.
	<b>Yes:</b> O.K.
	<b>No:</b> Continue with step 3.
3.	Click again on the header to sort the list in the reverse order.
	The sort can be in ascending or descending order, each time the user clicks on the same header again the list is sorted the other way.

1. Click on the header according to which the alarms are to be sorted.

*Response:* The alarms are sorted according to the selected alarm field in ascending or descending order.

2. Check if the list was sorted as desired.

**Yes:** O.K.

**No:** Continue with step 3.

3. Click again on the header to sort the list in the reverse order.

The sort can be in ascending or descending order, each time the user clicks on the same header again the list is sorted the other way.

### 6.3.4 System Management Functions

The general system management functions comprise the functions for file management, for defining view options and for getting help. These functions are contained in the following menus:

- File
- Views
- Filters
- Help.

#### 6.3.4.1 File

In the file menu you can start the following actions:

- New  
Launch a new instance of the Alarm Viewer.
- Reload  
Display a fresh copy of the current information shown in the window.
- Print  
(cf. Chapter 3.5, page 3-21).
- Close  
Close the active window, but without closing other instances of the Alarm Viewer. Same functionality as the Close button.
- Exit  
Close all Alarm Viewers opened by the user.

#### 6.3.4.2 Views

##### Summary

For displaying alarm lists you can select from four pre-defined views.

- View1:  
Index, Alarm Type, Host, Object Id, Severity, Status, Date&Time Last Change
- View2:  
Index, Alarm Type, Host, Object Id, Status, Date&Time First\_Raise, Date&Time Last\_Change, User Ack, Occurrences
- View3:  
Index, Summary, Host, Object ID, Severity, Status, Date&Time Last\_Change
- View4:  
All alarm fields.

##### Effects

The alarms are rearranged according to the selected criteria.

**Selecting Views**

Proceed as follows to select the desired view option:

Step	Procedure
1.	Select <b>Views</b> -> <b>ViewX</b> (X = 1 to 4) in the menu bar.  The same view options can be selected  — via the option menu <b>Views</b> in the general information section (cf. Chapter 6.3.3.3, page 6-14)  <i>Response:</i> The alarms are displayed according to the selected view.

**6.3.4.3 Filters****Summary**

For displaying the alarm lists you can select pre-defined filters. Only those alarms corresponding to the pre-defined criteria are displayed. The alarm set is displayed without modifying the current view.

The filters are:

- Alarms for the last 24 hours (all alarms which have been changed in the last 24 hours)
- Critical Raised Alarms
- Raised Alarms
- Alarms from a Host/s
- Critical Alarms not cleared
- Owned Acknowledge Alarms
- Clear Alarms
- All Acknowledge Alarms
- None Filter / All Alarms.

**Effects**

The alarms are rearranged according to the selected filter criteria.

**Selecting Filter**

Proceed as follows to select the desired filter option:

<b>Step</b>	<b>Procedure</b>
1.	Select the desired filter option:

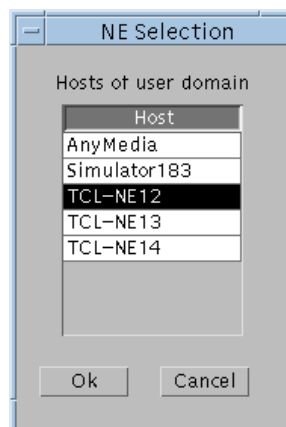
  

<b>If you want to view ...</b>	<b>then select <i>Filters</i> -&gt; ...</b>	<b>Result/Notes</b>
all alarms which have been changed in the last 24 hours	<b><i>Alarms for the last 24 hours</i></b>	The alarms are displayed according to the selected filter.
all critical raised alarms	<b><i>Critical Raised Alarms</i></b>	The alarms are displayed according to the selected filter.
all raised alarms	<b><i>Raised Alarms</i></b>	The alarms are displayed according to the selected filter.
all alarms from a host	<b><i>Alarms from a Host/s</i></b>	NE selection window will open, see details below.
all not cleared critical alarms	<b><i>Critical Alarms not cleared</i></b>	The alarms are displayed according to the selected filter.
all owned acknowledge alarms	<b><i>Owned Acknowledge Alarms</i></b>	The alarms are displayed according to the selected filter.
all cleared alarms	<b><i>Clear Alarms</i></b>	The alarms are displayed according to the selected filter.
all acknowledge alarms	<b><i>All Acknowledge Alarms</i></b>	The alarms are displayed according to the selected filter.
all alarms.	<b><i>None Filter / All Alarms</i></b>	The alarms are displayed according to the selected filter.

The same filter option can be selected

- via the option menu ***Filters*** in the general information section (cf. Chapter 6.3.3.3, page 6-14)

If you selected ***Alarms from a Host/s*** the NE selection window is displayed (cf. Figure 6-7, page 6-21) and you have to select one or more NEs and/or the AEM-NB for which the alarms should be displayed. Press ***OK*** in the NE selection window to display the alarms from the selected objects in the alarm viewer or press ***Cancel*** to cancel the operation.



**Figure 6-7 NE Selection Window**

#### 6.3.4.4 Help

Help is provided for every window. The help text describes the purpose of the window, how to use it and a description of each field of the window is given.

In the Menu Bar of each AEM-NB application there are two help options:

- Index  
Displays the help index, allowing the user to navigate through the AEM-NB help information.
- On window  
Displays the help information of the window where the user is currently working.

#### 6.3.5 Alarm Viewer Functions

##### Summary

The Alarm Viewer provides the user with different functions for managing alarm information:

- Manual or automatic reload of alarms
- Acknowledge alarms.  
The user can acknowledge one, more or all reported alarms. The AEM-NB allows different users to acknowledge the same alarm. The name of the last user who has acknowledged the alarm is stored.
- Clear alarms  
The user can clear one, more or all platform alarms. If not all selected alarms could be cleared, you are informed about the alarms for which this action failed.
- Print alarm lists (cf. Chapter 6.3.4.1, page 6-18).

**Prerequisites** Before performing alarm acknowledgment and alarm clearance select the alarms you want to acknowledge or clear.

**Starting Actions** Select the desired alarm viewer action:

If you want to ...	then select ...	Result/Notes
manually retrieve alarms	<b>File -&gt; Reload</b>	<p>Reloads alarms in the table. Only alarms which match the filter criteria are included. The Alarm Viewer is blocked until the reload is finished.</p> <p>Same functionality as <b>Reload</b> in the tool bar.</p> <p>To customize the displayed alarm list perform the actions described in Chapter 6.3.4.3, page 6-19 and Chapter 6.3.4.2, page 6-18.</p>
automatically update alarm view	<b>Options -&gt; Automatic Reload</b>	<p>If this menu item is checked, alarms are automatically reloaded in the alarm viewer every minute. If it is not checked, alarms are loaded only if <b>Reload</b> is pressed or if <b>File -&gt; Reload</b> is selected.</p> <p>The setting affects only the current window. The alarm viewer does not remember the setting after a restart.</p>
acknowledge alarms	<b>Actions -&gt; Acknowledge</b>	<p>All selected alarm items are acknowledged. Their status immediately changes to acknowledge.</p> <p>Same functionality as <b>Acknowledge</b> in the tool bar.</p> <p>For better readability the displayed alarms can be sorted (cf. Chapter 6.3.3.4.2, page 6-17).</p>
clear alarms	<b>Actions -&gt; Clear</b>	<p>All selected alarm items are cleared. Their status immediately changes to cleared.</p> <p>Same functionality as <b>Clear</b> in the tool bar.</p> <p>For better readability the displayed alarms can be sorted (cf. Chapter 6.3.3.4.2, page 6-17).</p>

## 6.4 Test Management

### Main Functions

The test management provides all the general purpose test functionality. The main functions are:

- Providing the user with different test options (see below),
- Starting the test execution by means of the AEM-NB,
- Displaying the test results on the AEM-NB user interface, and
- Setting and clearing of loopbacks.

### Test Options

The following test options are available:

- User Line Test (cf. Chapter 6.4.1, page 6-25)
- User Port test (cf. Chapter 6.4.2, page 6-29)
- Standby card test scheduling (cf. Chapter 6.4.3, page 6-31)
- Built-in self-test (cf. Chapter 6.4.4, page 6-32)
- TAP test (cf. Chapter 6.4.5, page 6-33)
- CRC test (cf. Chapter 6.4.6, page 6-34)
- Loopback test at the feeder side (cf. Chapter 6.4.7, page 6-37).

### Access to the Testroutines

The test routines are available via the "Configuration Manager" application. To start it, click **Config. Manager** in the Access Bar. The *Configuration Manager* window and the *Network Browser* pop up (cf. Figure 6-8, page 6-24).

### TL1 Commands

Some of the test routines can be executed via TL1 commands by using the TL1 command line interface (cf. Chapter 5.3.7).

Please refer to the AMAS R1.3 network elements documentation for a detailed description of TL1 commands (including an explanation of the input format, restrictions, error conditions etc.).

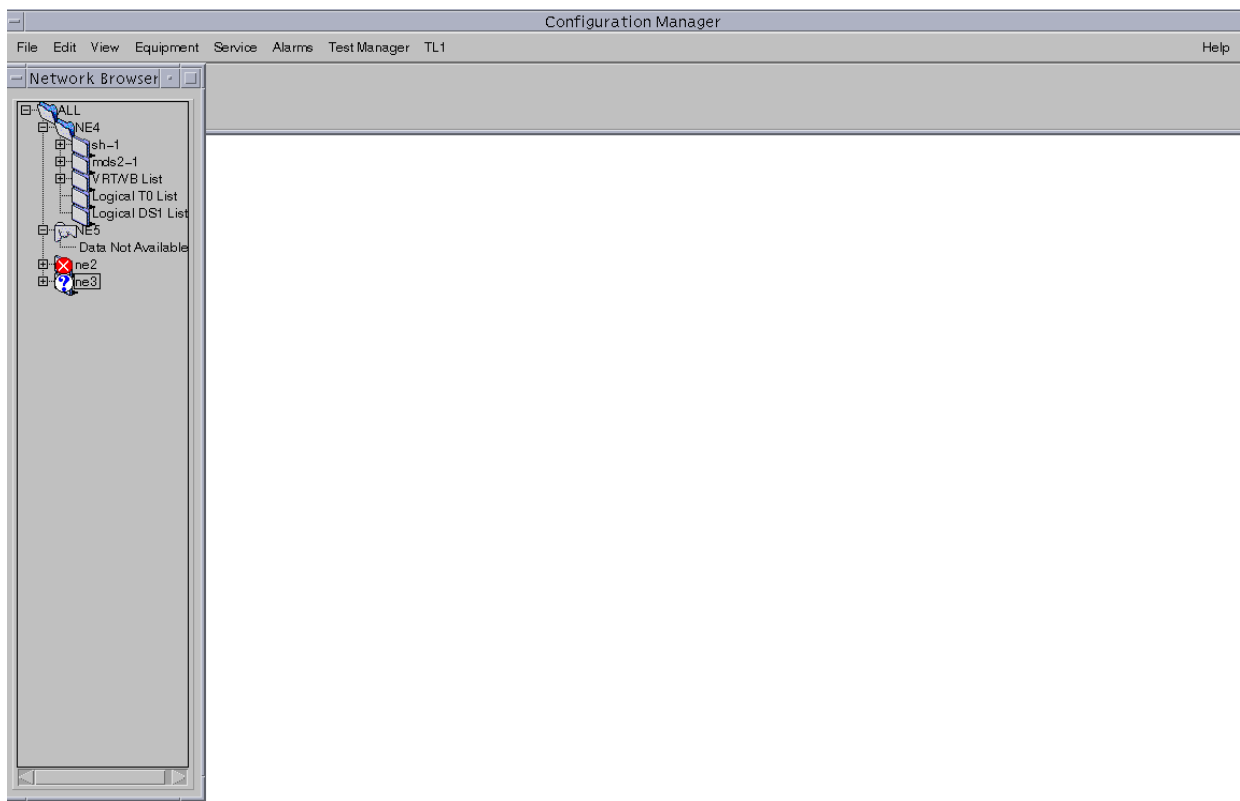


Figure 6-8 Window "Configuration Manager"



### 6.4.1 User Line Test

#### Precondition

Before a line test can be started the following must be done

- the TAP100 must be equipped and provisioned
- the connection between the TAP100 and the CIU must be established with the correct cable (from the front of the TAP100 to the backplane).

The AEM-NB automatically creates a line test entity when the TAP100 is equipped and provisioned.

#### Procedure

Proceed as follows to start a line test and view the test result:

Step	Procedure
------	-----------

1. Start the user line test.

You have the following options to do this:

- a. **Via the Network Browser and the menu bar:**

- Select the port you intend the test to run for in the Network Browser (**All -> NE -> Shelf -> LPZ100 (LPP100, LPU112) -> Drop id**).
- Start the test by selecting **Test Manager -> User Line Test** from the menu bar.

- b. **Via the Network Browser and the cursor menu:**

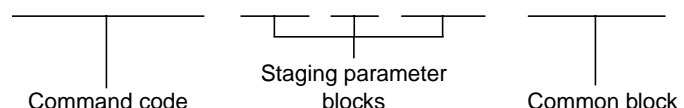
- Select the port you intend the test to run for in the Network Browser (**All -> NE -> Shelf -> LPZ100 (LPP100, LPU112) -> Drop id**).
- Start the test by selecting **Line Test** from the cursor menu.

- c. **Via the TL1 Command Line Interface:**

(This option does not open the *Line Test Result* window; cf. step 2.)

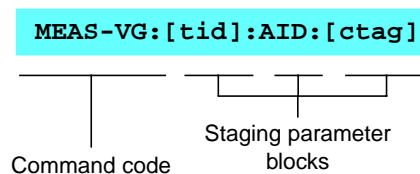
Enter the following TL1 command to start the line test:

```
CONN-TACC-DROP:[tid]:AID:[ctag]::[TESTMODE];
```

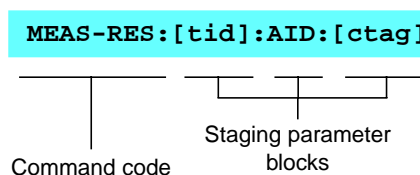


The single measurements has to be started separately.

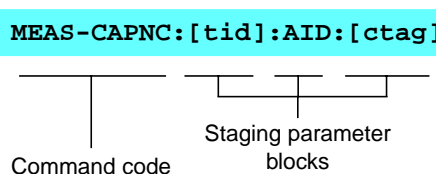
For voltage measurement:



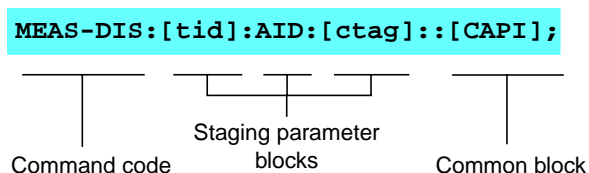
For resistance measurement:



For capacitance measurement:



For distance measurement:



2. Wait until the *Line Test Result* window (cf. Figure 6-9, page 6-27) appears and view the test result.



**NOTE:**

After confirming the user line test execution a *In Progress* window pops up showing the following message:

**User Line Test execution in progress on NE Name, Slot, Card Type, Port id.**

Clicking on the *Cancel* button will stop the test and the result window (see below) will not appear.

**Test Result**

The *Line Test Result* window shows the test results of a series of self-diagnostic routines on a specific port circuit.

The screenshot shows the 'Line Test Result' window with the following data:

Field	Value
NE Name	TCL-NE14
Slot	ap-1-6
Provisioned Apparatus Code	LPP100
Port id	drop-1-6-1

Test Type	Measurement	Value	Unit
AC Voltage	A against B	0	Vms
	A against Ground	0	Vms
	B against Ground	0	Vms
DC Voltage	A against B	0	Vdc
	A against Ground	0	Vdc
	B against Ground	0	Vdc
Resistance	A against B	16000000	Ohm
	A against Ground	16000	KOhm
	B against Ground	16000	KOhm
	A/B against Ground	8000	KOhm
	A against Battery	16000	KOhm
	B against Battery	16000	KOhm
Capacitance	A against B	20	nF
	A against Ground	20	nF
	B against Ground	20	nF
Distance to open	Distance	0.5	Km
	Capacitance	20	nF

Close

**Figure 6-9** The "Line Test Result" Window

The text fields are display-only, they have the following meaning:

**Table 6-11** Meaning of the Text Fields in the "Line Test Result" Window

Text Fields	Meaning	Possible Values
<b>NE Name</b>	The unique identifier of the selected NE as specified at NE creation time.	Any string consisting of up to 30 characters
<b>Slot</b>	The slot number of the AP being used.	ap-1-{1, 16}
<b>Provisioned Apparatus Code</b>	Mnemonic used to identify the general type of function provided (AP card type).	LPZ100 (LPP100, LPU112 (cf. Chapter 5.3.3.2)
<b>Port id</b>	The drop within the AP.	drop-1-{1, 16}-{1, 32}

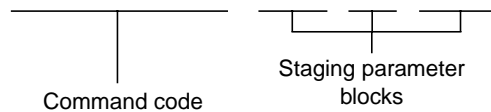
**Table 6-11** Meaning of the Text Fields in the "Line Test Result" Window

Text Fields	Meaning	Possible Values
<b>AC Voltage (Vrm)</b>	Results of the AC measurements.	0 to 200 Vrms.
<b>DC Voltage (Vdc)</b>	Results of the DC measurements.	-150 to 150 Vdc.
<b>Resistance (Ohm)</b>	Results of the isolation resistance measurements.	0 to 16000 kOhm (0 to 8000 kOhm for A/B against Ground)
<b>Capacitance (nF)</b>	Results of the capacitance measurements.	20 to 9000 nF
<b>Distance to open</b>	Results of the distance measurements.	0.5 to 30 km for distance 20 to 9000 nF for capacitance.

Click on **Close** to exit the *Line Test Result* window.

To stop the test session via TL1 command proceed as follows:

**DISC-TACC-DROP:[tid]:AID:[ctag];**



## 6.4.2 User Port Test

**Purpose** By means of a port test you are able to run a series of self-diagnostic routines for a particular port on a specified AP.

**Procedure** Proceed as follows to start a port test and view the test result:

Step	Procedure
------	-----------

1.	Start the port test.
----	----------------------

You have the following options to do this:

**Procedure via Menu Bar**

a. **Via the Network Browser and the menu bar:**

- Select the port you intend the test to run for in the Network Browser (**All -> NE -> Shelf -> LPZ100 (LPP100, LPU112, TAP100) -> Drop id**).
- Start the test by selecting **Test Manager -> User Port Test** from the menu bar.

**Procedure via Cursor Menu**

b. **Via the Network Browser and the cursor menu:**

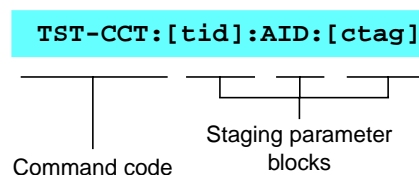
- Select the port you intend the test to run for in the Network Browser (**All -> NE -> Shelf -> LPZ100 (LPP100, LPU112, TAP100) -> Drop id**).
- Start the test by selecting **User Port Test** from the cursor menu.

**Procedure via TL1 Command**

c. **Via the TL1 Command Line Interface:**

(This option does not open the *Port Test Result* window; cf. step 2.)

Enter the following TL1 command by using the TL1 command line interface (cf. Chapter 5.3.7):



This command starts an AP self test for the specified drop. For this test, no test line and active test session is needed. Nevertheless, if a test session is active, only the drop circuit of the test session can be tested if the test session mode is set to "Manual" or "Integrated". If the drop is not accessible by the system, the test is denied. The served service, if any, of the drop must allow a disruption of the service during the circuit test. If needed and if possible, the service will be blocked in cooperation with the connected exchange by this command. If the circuit of a test AP is tested by this command, the test AP performs a self test and a calibration.

2. Wait until the *Port Test Result* window (cf. Figure 6-10, page 6-30) appears and view the test result.

**NOTE:**

After confirming the user port test execution a *In Progress* window pops up showing the following message:

**Port Test execution in progress on NE Name, Slot, Card Type, Port id.**

Clicking on the *Cancel* button will stop the test and the result window (see below) will not appear.

**Test Result**

The *Port Test Result* window shows the test results of a series of self-diagnostic routines on a specific port circuit.

Port Test Result	
NE Name	TCL-NE14
Slot	ap-1-6
Provisioned Apparatus Code	LPP100
Port id	drop-1-6-1
Result	Passed
<div>Close</div>	

**Figure 6-10** The "Port Test Result" Window

The text fields are display-only, they have the following meaning:

**Table 6-12 Meaning of the Text Fields in the "Port Test Result" Window**

Text Fields	Meaning	Possible Values
<b>NE Name</b>	The unique identifier of the selected NE as specified at NE creation time.	Any string consisting of up to 30 characters
<b>Slot</b>	The slot number of the AP being used.	ap-1-{1, 16}
<b>Provisioned Apparatus Code</b>	Mnemonic used to identify the general type of function provided (AP card type).	LPZ100, LPP100, LPU112, TAP100 (cf. Chapter 5.3.3.2)
<b>Port id</b>	The port within the AP.	drop-1-{1, 16}-{1, 32}
<b>Result</b>	The result of the test routines.	PASS or FAIL

Click on **Close** to exit the *Port Test Result* window.

### 6.4.3 Standby Card Test Scheduling

#### Side Switch and Off-Line Diagnostics Possible User Settings

During the execution of a standby card test scheduling a COMDAC side switch and off-line diagnostics for the standby COMDAC is performed.

The AEM-NB provides the opportunity to the user to set-up the periodicity and the time of the day (cf. Table 6-13, page 6-32) to perform a standby card test over:

- the standby COMDAC.

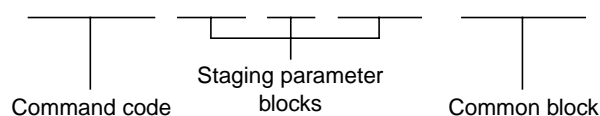
#### Procedure

Proceed as follows to start the card test scheduling:

Step	Procedure
------	-----------

- |    |  |
|----|--|
| 1. | To schedule a standby card test enter the following TL1 command by using the TL1 command line interface (cf. Chapter 5.3.7): |
|----|--|

**SCHED-EX:[tid]:AID:[ctag]::INVL,STM**



The SCHED-EX (Schedule-Exercise) command instructs the system to set up an exercise schedule (exercise interval and start time of the day of exercise) to perform a COMDAC side switch or off-line diagnostics for the standby COMDAC.

**Parameters in the Common Block**

The parameters in the common block have the following meaning:

**Table 6-13 Common Block Parameters for SCHED-EX**

Parameter	Meaning	Format	Possible Values
<b>INVL</b> (Interval)	Periodicity: The number of days between two standby card tests.	x-DAY	x=1 ... 365
<b>STM</b> (Start Time)	The time of the day when standby card tests shall be performed.	hh-mm	hh=0 ... 23 (hour-of-day) mm=0 ... 59 (minute-of-hour).

Please refer to the AMAS R1.3 network elements documentation for a detailed description of TL1 commands (including an explanation of the input format, restrictions, error conditions etc.).

**Result**

Depending on the standby card test result the following behaviour can be observed:

- If the test is successful the side switch will be performed.
- If the test fails then no side switch will be performed. Additionally an alarm will be raised in this case.

**6.4.4 Built-in Self-Test****Test Request**

Each NE performs a built-in self-test of plug-ins periodically.

**NOTE:**

The built-in self-test is not requested from the AEM-NB, it will be always started from the NE!

**Procedure**

If a failure occurs, the NE will raise an alarm (*REPT-ALM*) which contains the AID of the failed plug-in. The alarm is then visible in the "Alarm Viewer" of the AEM-NB. For more information about possible alarms see Chapter 6.6.4, page 6-46 (describes AEM-NB alarms) or refer to the AMAS R1.3 network elements documentation (describes NE alarms).



### 6.4.5 TAP-Test

This command starts a test access point wiring consistency test which checks the correct cabling between the CIU and the test AP. This test is only allowed without an active test session.

The AEM-NB automatically creates a line test entity when the TAP100 is equipped and provisioned.

## Procedure

Proceed as follows to start a TAP test and view the test result:

Step	Procedure
1.	<p>Start the TAP test.</p> <p>You have the following options to do this:</p> <ul style="list-style-type: none"><li>a. <b>Via the Network Browser and the menu bar:</b><ul style="list-style-type: none"><li>— Select the port you intend the test to run for in the Network Browser (<b>All -&gt; NE -&gt; Shelf -&gt; TAP100</b>).</li><li>— Start the test by selecting <b>Test Manager -&gt; TAP Test</b> from the menu bar.</li></ul></li><li>b. <b>Via the Network Browser and the cursor menu:</b><ul style="list-style-type: none"><li>— Select the port you intend the test to run for in the Network Browser (<b>All -&gt; NE -&gt; Shelf -&gt; TAP100</b>).</li><li>— Start the test by selecting <b>TAP Test</b> from the cursor menu.</li></ul></li><li>c. <b>Via the TL1 Command Line Interface:</b><p>(This option does not open the <i>TAP Test Result</i> window; cf. step 2.)</p><p>Enter the following TL1 command to start the TAP test:</p></li></ul>

```
TST-TAP:[tid]::[ctag];
```

Command code

### Staging parameter blocks

- Wait until the *TAP Test Result* window (cf. Figure 6-11, page 6-34) appears and view the test result.

**⇒ NOTE:**

NOTE:  
After confirming the TAP test execution a *In Progress* window pops up showing the following message:

TAP Test execution in progress on *NE Name, Slot*.

Clicking on the *Cancel* button will stop the test and the result window (see below) will not appear.

**Test Result**

The *TAP Test Result* window shows the test results of a series of self-diagnostic routines on a specific port circuit.

**Figure 6-11 The "TAP Test Result" Window**

The text fields are display-only, they have the following meaning:

**Table 6-14 Meaning of the Text Fields in the "TAP Test Result" Window**

Text Fields	Meaning	Possible Values
<b>NE Name</b>	The unique identifier of the selected NE.	Any string consisting of up to 30 characters
<b>Slot</b>	The slot number of the Application Pack being used.	ap-1-{1, 16}
<b>Provisioned Apparatus Code</b>	Mnemonic used to identify the type of card provided.	TAP100
<b>Result</b>	The result of the test routines.	PASS or FAIL.

3. Click on **Close** to exit the *TAP Test Result* window.

### 6.4.6 CRC Test

This command starts a CRC test procedure for the specified ISDN drop. The CRC test procedure checks the proper functionality of the CRC generator and detector for the specified time period.

**Precondition**

Before the CRC test can be started an ISDN telephone must be connected to the port which shall be tested.

**Procedure**

Proceed as follows to start a CRC test and view the test result:

Step	Procedure
------	-----------

1.	Start the CRC test.
----	---------------------

You have the following options to do this:

**Procedure via Menu Bar**

a. **Via the Network Browser and the menu bar:**

- Select the port you intend the test to run for in the Network Browser (**All -> NE -> Shelf -> LPU112**).
- Start the test by selecting **Test Manager -> CRC Test** from the cursor menu. The *CRC Test* window pops up:

**Figure 6-12 "CRC Test" Window**

The text fields are display-only, they have the following meaning:

**Table 6-15 Meaning of the Text Fields in the "CRC Test" Window**

Text Fields	Meaning	Possible Values
<b>NE Name</b>	The unique identifier of the selected NE.	Any string consisting of up to 30 characters
<b>Slot</b>	The slot number of the AP being used.	ap-1-{1, 16}
<b>Provisioned Apparatus Code</b>	Mnemonic used to identify the general type of function provided.	LPU112
<b>Port id</b>	Identifies the selected drop within the AP.	drop-1-{1, 16}-{1, 32}.
<b>Test Programming</b>	<p>The option menu <b>Directionality</b> can be used to define the direction of the test.</p> <p>The option menu <b>Test Duration</b> can be used to define the test duration in seconds.</p>	<p>Up and Down</p> <p>1 ... 15, step1</p>
<b>Test Results</b>	<p>The field <b>Test Results</b> shows the general test result</p> <p>The field <b>CRC Errors Per Second</b> shows the number of detected CRC errors per second.</p>	<p>CRC-FAIL, CRC-OK</p> <p>0 ... 100, step 1</p>

2. Use the option menus in the pane **Test Programming** to define test parameters.
3. Click on **Apply** to confirm. A *In Progress* window pops up showing the following message:

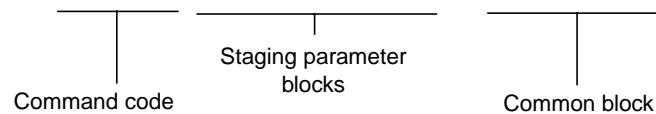
**CRC Test execution in progress on NE Name, Slot, Card Type, Port id.**

#### Test Result

4. Wait until the **Test Results** appears (cf. Figure 6-12, page 6-35) and view the test result.

**Procedure via TL1 Command****b. Via the TL1 Command Line Interface:**

```
TST-CRC:[tid]:AID:[ctag]::[DIRN][,SEC];
```



Wait until the *CRC Test* window appears (cf. Figure 6-12, page 6-35) and view the test result.

**NOTE:**

After confirming the CRC test execution a *In Progress* window pops up showing the following message:

**CRC Test execution in progress on NE Name, Slot, Card Type, Port id.**

Clicking on the *Cancel* button will stop the test and the test result fields in the CRC Test window (see below) will be cleaned.

**Test Result**

The *CRC Test* window (pane **Test Results** - cf. Figure 6-12, page 6-35) shows the test results of a series of self-diagnostic routines on a specific port circuit.

### 6.4.7 Loopback Test at the Feeder Side

It is possible to set or clear a loopback on particular feeders.

**Procedure**

Proceed as follows to set/clear E1 loopbacks:

Step	Procedure
------	-----------

You have the following options to set/clear a loopback:

**Procedure via Network Browser****a. Via the Network Browser and the menu bar:**

1. Select the E1 Feeder you intend the test to run for in the Network Browser (**All -> NE -> Shelf -> FAC500 -> E1 Feeder**) and **Edit** via the cursor menu.

The *E1 Feeder/V5 Link* window pops up (tab E1 Feeder). The **Loopback** field displays the current loopback state (**Clear** or **Set**).

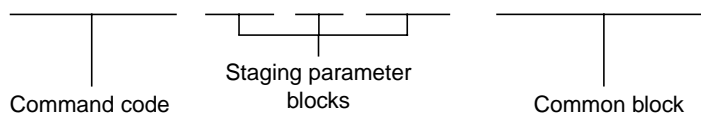
2. Click **Label** to change the loopback state.

Depending on the loopback state reflected, this command button displays the possible operation (**Clear**, if the loopback is set; **Set**, if the loopback is cleared).

b. **Via the TL1 Command Line Interface:**

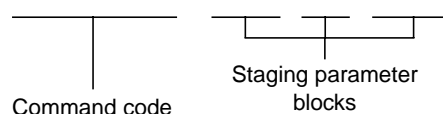
To **set** a loopback enter the following TL1 command by using the TL1 command line interface (cf. Chapter 5.3.7):

```
OPR-LPBK-E1:[tid]:AID:[ctag]::[LPKTYPE][MODE];
```



To **clear** a loopback enter the following TL1 command by using the TL1 command line interface:

```
RLS-LPBK-E1:[tid]:AID:[ctag];
```



## 6.4.8 Loopback Test at the ISDN User Port Side

It is possible to set or clear a loopback on an ISDN drop.



**NOTE:**

DLL loopbacks can not be done by the AEM-NB. It is only possible via GSI.

### Set Procedure

Proceed as follows to set a loopback test at the ISDN User Port side:

Step	Procedure
------	-----------

You have the following options to do this:

### Procedure via Menu Bar

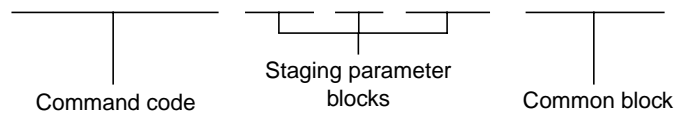
a. **Via the Network Browser and the menu bar:**

1. Select the port you intend the test to run for in the Network Browser (**All -> NE -> Shelf -> LPU112 -> Drop id (ISDN)**) and **Edit** via the cursor menu  
or select **File -> Open** or **Service -> Provisioning -> Edit/View** via the menu bar. The *V5 ISDN-BRA User Port* window pops up.
2. Use the option menu **Loopback Selection** to select the set loopback option and click on **Request**.

**Procedure via TL1****b. Via the TL1 Command Line Interface:**

To set a loopback enter the following TL1 command by using the TL1 command line interface:

```
OPR-LPBK-ISDN:[tid]:AID:[ctag]::[LPKTYPE];
```



This command operates a loopback on an ISDN drop.

If the drop serves an ISDN basic rate access subscriber the subscriber is blocked in cooperation with the connected exchange by this command. In case of serving a digital leased line subscriber the loopback is switched transparently through the system towards the service node if the cross-connection is provisioned and all involved entities are operational. If the drop is not accessible by the system, the requested loopback is already active or the drop is currently under test the loopback is denied.

The loopback will be automatically released when a user is entered on the drop, the administrative service state of the user is changed, a integrated test on the drop is started, the connected exchange unblocks the ISDN basic rate access subscriber or in case of any hardware faults of the related AP.

**Clear Procedure**

Proceed as follows to clear a loopback test at the ISDN User Port side:

Step	Procedure
------	-----------

You have the following options to do this:

**Procedure via Menu Bar****a. Via the Network Browser and the menu bar:**

1. Select the port you intend the test to run for in the Network Browser (**All -> NE -> Shelf -> LPU112 -> Drop id (ISDN)**) and **Edit** via the cursor menu or select **File -> Open** or **Service -> Provisioning -> Edit/View** via the menu bar. The *V5 ISDN-BRA User Port* window pops up.
2. Use the option menu **Loopback Selection** to select the clear loopback option and click on **Request**.

**Procedure via TL1****b. Via the TL1 Command Line Interface:**

To clear a loopback enter the following TL1 command by using the TL1 command line interface (cf. Chapter 5.3.7)::

```
RLS-LPBK-ISDN:[tid]:AID:[ctag];
```



## 6.5 Information Management and Maintenance

---

### 6.5.1 NE-AEM-NB Connection States

---

#### Connection States

There are five NE-AEM-NB connection states. They depend on the availability of a TCP/IP connection and TL1 communication session between the AEM-NB and NE and also on the AEM-NB's attempt to open a TL1 communication session with the NE:

- NOT\_CONNECTED

Initial NE state when there is no connection between AEM-NB and NE and the AEM-NB is in a "passive" state avoiding any possibility of connection establishment with the NE.

- NOT\_CONNECTED (TRYING)

Initial NE connection establishment state when the TL1 communication session between the AEM-NB and NE is not available (AEM-NB login to NE via ACT-USER command) but the AEM-NB is in an "active" state trying to open a connection (TCP/IP connection and TL1 communication session) with the NE.

- NOT\_CONNECTED (CANCELLING)

The communication session between the AEM-NB and NE is available but the AEM-NB is trying to close connection (TCP/IP connection and communication session) with NE. The user is unavailable to execute any action.

- CONNECTED (SYNCHRONIZING)

The communication session between the AEM-NB and NE is available but the AEM-NB is trying to synchronize AEM-NB and NE information. The user is unavailable to execute any action until the synchronizing process is finished. After that the state changes to CONNECTED.

- CONNECTED

TL1 communication session between the AEM-NB and NE is available (TCP/IP connection is alive) and the software version currently stored in the NE is supported by the AEM-NB. When the association process between the AEM-NB and NE is completed, the NE state changes to CONNECTED and remains like this until the TL1 communication session is closed on user request or the TCP/IP connection is lost/closed.

### 6.5.2 Changing Connection States

---

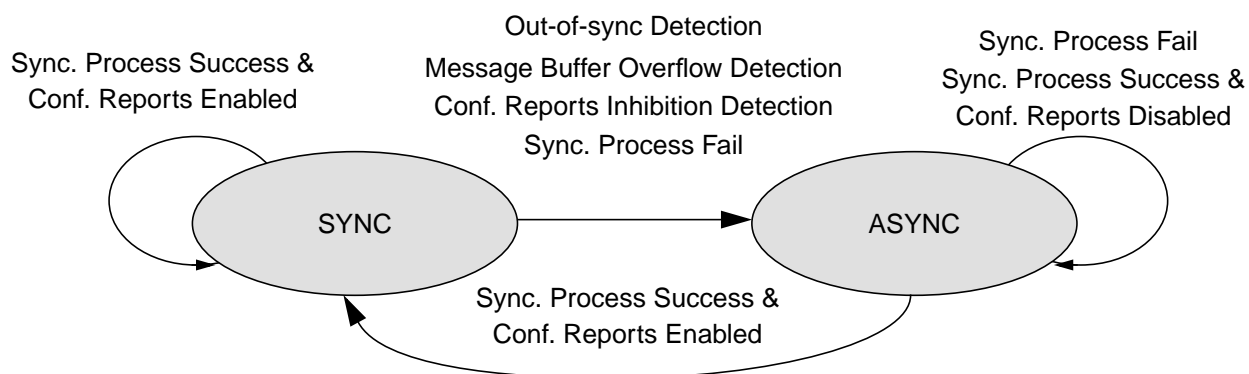
The connection state changes can be initiated by the user via the GUI (cf. Chapter 5.3.1, page 5-17, section „Connect NE“) or they are initiated by the AEM-NB.



<b>Not Connected</b>	The user can initiate the connection establishment process with an NE in connection state NOT_CONNECTED. After initiating this process the NE state changes to NOT_CONNECTED (TRYING).
<b>Not Connected (Trying)</b>	When the NE state is NOT_CONNECTED (TRYING), the AEM-NB tries to establish a TCP/IP connection with the NE. The AEM-NB attempts to connect to one of the TCP ports of the NE. After the successful connection to a TCP port, the AEM-NB checks if it supports the software version of the NE. If the software version is supported the NE state becomes CONNECTED (SYNCHRONIZING), if not it remains NOT_CONNECTED (TRYING) and the AEM-NB continues its attempts to establish a connection. The user can cancel these attempts via the GUI, which will change the NE state to NOT_CONNECTED (CANCELLING).
<b>Connected</b>	The user can request to close a connection with an NE via the GUI. When the TL1 communication session is closed by the AEM-NB, the NE state is changed to NOT_CONNECTED. When the NE state is CONNECTED and the TCP/IP connection is lost or closed, the NE state becomes NOT_CONNECTED (TRYING). When a TL1 communication session loss is detected and the TCP/IP connection is still established, the AEM-NB closes the TCP/IP connection and the NE state also becomes NOT_CONNECTED (TRYING).

### 6.5.3 Configuration Data Synchronization after Association

<b>General</b>	If an NE is connected to the AEM-NB the databases of NE and AEM-NB have to be synchronized. To change synchronization settings see Chapter 5.3.3.1, page 5-45.
<b>Autonomous Reports</b>	There are various types of autonomous reports that are used to keep consistency between configuration changes in the NE and AEM-NB database (e.g. LED status reports, switch reports). For an NE the user can disable the sending of autonomous reports (reports can be inhibited/enabled separately or collectively). But to maintain consistency between the NE configuration data and the AEM-NB database, these configuration reports have to be enabled.
<b>Synchronization States Diagram</b>	The following figure illustrates the NE state model depending on the synchronization state between the data kept in the NE and the AEM-NB database.



**Figure 6-13 NE Configuration Data Synchronization States**

#### SYNC/ASYNC

There are the following two NE configuration data synchronization states:

- SYNC

The AEM-NB database is consistent with the locally stored NE information, and all the autonomous messages concerning configuration changes are enabled (configuration reports: database changes, LED status reports, switch reports and some events of the type protection switching and inhibit messages).

- ASYNC

The AEM-NB database and the NE configuration data are out of synchronization and/or configuration reports are inhibited and/or the AEM-NB configuration messages buffer is overflowed.

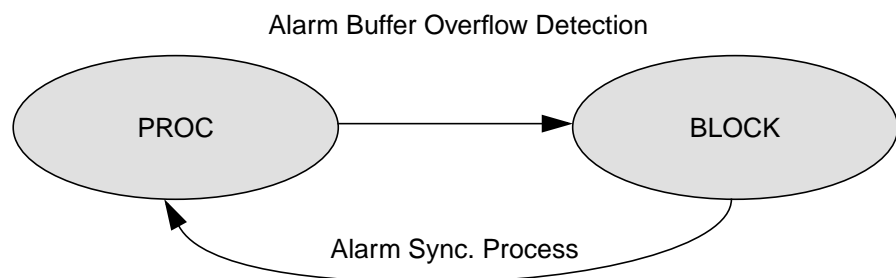
#### 6.5.4 Alarm Data Synchronization after Association

##### Alarm Data

The AEM-NB maintains alarm data for each NE. These data are updated with all NE alarms and environment alarms from the NEs database. To change synchronization settings see Chapter 5.3.3.1, page 5-45.

##### Synchronization States Diagram

The following figure illustrates the NE state model depending on the synchronization state between the alarm data kept in the NE and the AEM-NB alarm database.



**Figure 6-14 NE Alarm Data Synchronization States**

#### PROC/BLOCK

There are two NE alarm synchronization states:

- **PROC**

The AEM-NB alarm database is consistent with the current NE alarms. If alarm and/or environment alarm reports are inhibited, the AEM-NB database is only a snapshot of NE alarm information at a certain moment in time.

- **BLOCK**

The AEM-NB alarm database and the current NE alarms are out of synchronization due to an alarm buffer overflow. The AEM-NB alarm database is only a snapshot of NE alarm information at a certain moment in time.

#### Configuration Data

The AEM-NB configuration data which are maintained for each NE are updated with the NEs configuration data. The data from the NE non-volatile data storage (NVDS) are used.

### 6.5.5 Association Maintenance

#### Association

An association between the AEM-NB and an NE is established if the TCP/IP connection and the TL1 communication session are opened. The NE state changes into CONNECTED.

#### NE Monitoring

The AEM-NB monitors the association state of the NE by periodically sending messages (RTRV-HDR) to the NE. If the AEM-NB does not receive a response to a certain number of messages within a certain time, it assumes that the TL1 connection to the NE is lost and closes the TCP/IP connection to the NE.

#### Default Values for Monitoring

By default these messages are sent by the AEM-NB every five minutes. The response to a message must be received within four minutes and not more than two responses may be lost, otherwise the TCP/IP connection is closed by the AEM-NB.

These values can be configured by the user via the system variables "NEM.association.heartBeatNumber" and "NEM.association.heartBeatTime" in the file \$ANYMEDIAPATH/cfg/AnyMediaNBEM.cfg.

## 6.6 Alarms

### 6.6.1 Overview

An alarm is reported for any condition that needs user attention, since it may impact the normal operations of any system under user responsibility (e.g. AEM-NB, NE).

### 6.6.2 Alarm Types

#### Alarm Classification

Detected alarms are classified as one of the following:

- Platform Alarm

Alarm related to the AEM-NB application or its hardware/software platform. Generated (raised) by any object of the AEM-NB when it detects an abnormal condition to be reported to the user.

Information provided:

- AEM-NB Object Identifier
- Alarm Type Identifier
- Severity
- Service Affecting
- Occurrence Time.

- NE-AM Alarms

Generated (raised) by the NE-AM. Refer to Chapter 6.2.5, page 6-7 to see how the information comes from the NE-AM to the AEM-NB. The NE-AM alarms are classified in two groups:

- Normal Alarms

Data provided:

Access Identifier, Condition Type, Notification Code, Service Affecting, Access Identifier Type, Occurrence Date, Occurrence Time

- Environment Alarms

Data provided:

Access Identifier, Alarm Type, Notification Code, Occurrence Date, Occurrence Time

For all alarm types several alarm data fields are conceptually the same (although they convey different values). For instance, both Condition Type and Alarm Type refer to the type of alarm being raised/cleared (Battery on discharge, Loss of frame, ...).

The following table maps all the equivalent fields to general names that uniquely identify a concept independently of the alarm type.

**Table 6-16 General Alarm Fields**

General Name	Platform Alarm	NE Alarm	NE Environment Alarm
Object_Id.	EM Object Identifier	Access Identifier	Access Identifier
Alarm_Type	Alarm Type Identifier	Condition Type	Alarm Type
Severity	Severity	Notification Code	Notification Code
Serv_Affec.	Service Affecting	Service Effect	-
Date_First_Time/ Date_Last_Time <sup>a</sup>	Occurrence Time and Date <sup>a</sup>	Occurrence Time <sup>b</sup>	Occurrence Time <sup>b</sup>
		Occurrence Date <sup>c</sup>	Occurrence Date <sup>c</sup>

a Time and date (YYYY-MM-DD HH-MM-SS)

b Only time (HH-MM-SS)

c Only date (MM-DD)

#### Alarm Severities

For each alarm one of the following alarm severities is defined:

- Critical (CR)
- Major (MJ)
- Minor (MN)
- Information (IN), only applicable for platform alarms.

#### Alarm Identification

The multiple key that uniquely identifies an alarm is:

- Host Identifier  
Identifies where the alarm comes from. If it comes from an NE, then this identifier is the NE name. If the alarm is reported by the AEM-NB the host identifier is "EM". For association alarms the host identifier is "NE\_name".
- System Object Identifier  
Identifies the alarm-affected object within the host, which is identified by the host identifier. For association alarms the system object identifier is "ASSOC".
- General Alarm Identifier.  
Unique identifier within each type of alarm.

In order to ease possible communication between different users, an index number is provided as a temporal alarm identification. It is temporal because the index number will be used as a circular sequence (the maximum sequence number is 100 000). It is provided only for user convenience. It will not be used to identify an alarm within the AMS. For this purpose the multiple key defined above has to be used.

### 6.6.3 Network Element Alarms

**Alarm Descriptions** Please refer to the AMAS R1.3 network element documentation for detailed alarm descriptions of network element alarms.

### 6.6.4 Element Manager Platform Alarms

This chapter provides alarm descriptions of the AEM-NB platform alarms including proposals for corrective maintenance actions.

**Alphabetical Order** In the following the AEM-NB platform alarms are listed alphabetically.

#### 6.6.4.1 LOG\_DEL\_FULL

**Meaning** All old logs have been deleted. Because more available space was necessary the log type of the current day has been deleted, too. The Object\_Id shows which log type has been deleted.

**Abbreviation:** LOG\_DEL\_FULL

**Severity:** Major

**Service affecting:** No

**Effects** There are no old logs available, and not all logs of the current day are available to be viewed or stored.

**Possible Cause(s)** There may be a problem or abnormal situation in the AEM-NB, or the selection of the configurable size limits of the log system was too small.

**Corrective Actions** Proceed as follows to clear the alarm:

Step	Procedure
1.	<p>Check the AEM-NB for problems or abnormal situations.</p> <p>Have there any problems or abnormal situations occurred?</p> <p><b>Yes:</b> Try to resolve these problems or abnormal situations. If this is not possible, continue with step 2.</p> <p><b>No:</b> Continue with step 2.</p>
2.	<p>Check the size limits of the log system.</p> <p>Are the size limits set correctly (cf. Chapter 3.7.2, page 3-31)?</p> <p><b>Yes:</b> Call Lucent Technologies Technical Support.</p> <p><b>No:</b> Set the size limits correctly, i.e. increase the size limits.</p>

**6.6.4.2 LOG\_DEL\_PART**

**Meaning** A log type not yet archived has been deleted due to lack of available space.

**Abbreviation:** LOG\_DEL\_PART

**Severity:** Minor

**Service affecting:** No

**Effects** The respective log type can neither be viewed nor archived.

**Possible Cause(s)** There may be a problem or an abnormal situation in the AEM-NB, or the configurable size limits of the log system have not been chosen correctly.

**Corrective Actions** Proceed as follows to clear the alarm:

Step	Procedure
1.	Archive the remaining logs to prevent them from being deleted.
2.	Check the AEM-NB for problems or abnormal situations.  Have there any problems or abnormal situations occurred?  <div style="margin-left: 40px;"> <b>Yes:</b> Try to resolve these problems or abnormal situations. If this is not possible, continue with step 3.   <b>No:</b> Continue with step 3. </div>
3.	Check the size limits of the log system.  Are the size limits set correctly (cf. Chapter 3.7.2, page 3-31)?  <div style="margin-left: 40px;"> <b>Yes:</b> Call Lucent Technologies Technical Support.   <b>No:</b> Set the size limits correctly, i.e. increase the size limits. </div>

**6.6.4.3 NEASSOC\_FAILED**

**Meaning** The communication association with the NE has failed.

**Abbreviation:.** NE\_ASSOC\_FAILED

**Severity:.** Minor

**Service affecting:.** No

This alarm covers the the following alarms:

- TCP/IP\_CON\_REFUSED (cf. Chapter 6.6.4.6, page 6-49)
- TL1\_COMM\_DENIED (cf. Chapter 6.6.4.7, page 6-50)
- NEASSOC\_LOST (cf. Chapter 6.6.4.4, page 6-48).



**NOTE:**  
This alarm is only used in pass-through applications.

#### 6.6.4.4 NEASSOC\_LOST

<b>Meaning</b>	The AEM-NB lost the management association with the network element (NE).
<b>Abbreviation:</b>	NEASSOC_LOST
<b>Severity:</b>	Critical
<b>Service affecting:</b>	No
	The alarm will be cleared when the TCP/IP connection and TL1 communication session are available, and the software version currently stored in the NE is supported by the AEM-NB, i.e. when the association process between the AEM-NB and the NE is completed (NE state is <b>CONNECTED</b> , cf. Chapter 6.5.1, page 6-40).
<b>Effects</b>	It is not possible to manage the NE. The TL1 communication session and the TCP/IP connection are lost.
<b>Possible Cause(s)</b>	A loss of the TCP/IP connection has been detected, or the TCP/IP connection has been closed as a consequence of a loss of the TL1 communication session.
<b>Corrective Actions</b>	Proceed as follows to clear the alarm:

Step	Procedure
1.	<p>Check the NE state after a waiting period of 1 minute.</p> <p><i>Comment:</i> When NE state is <b>CONNECTED</b> and the TCP/IP connection is lost or closed, the NE state is moved to <b>TRYING</b> and the loop process to re-establish the connection with the NE is started by the AEM-NB.</p> <p>Is the state <b>CONNECTED</b>?</p> <p><b>Yes:</b> O.K.</p> <p><b>No:</b> Continue with step 2.</p>
2.	<p>Check for Data Communication Network (DCN) being in service.</p> <p>Is the DCN in service?</p> <p><b>Yes:</b> Call Lucent Technologies Technical Support.</p> <p><b>No:</b> Put the DCN into service.</p>



**6.6.4.5 SWVR\_ILLEGAL**

**Meaning** The Software Version currently stored in the NE is not supported by the AEM-NB.

**Abbreviation:** SWVR\_ILLEGAL

**Severity:** Critical

**Service affecting:** No

**Effects** It is not possible to manage the NE.

**Possible Cause(s)** The Software Version currently stored in the NE is not supported by the AEM-NB.

**Corrective Actions** Proceed as follows to clear the alarm:

---

Step	Procedure
------	-----------

---

- |    |  |
|----|--|
| 1. | Check that the correct version of software is installed on the NE's System Controller Card (COMDAC). |
|----|--|

**6.6.4.6 TCP/IP\_CON\_REFUSED**

**Meaning** The TCP/IP connection establishment could not be completed successfully for port numbers 11002, 11004, 11006 and 11008.

**Abbreviation:** TCP/IP\_CON\_REFUSED

**Severity:** Critical

**Service affecting:** No

**Effects** It is not possible to manage the NE.

**Possible Cause(s)** Some TCP/IP protocol errors stopped the connection establishment process between AEM-NB and NE.

**Corrective Actions** Proceed as follows to clear the alarm:

---

Step	Procedure
------	-----------

---

- |    |  |
|----|--|
| 1. | Check the TCP/IP communication addresses.<br><br>Are the TCP/IP communication addresses correct?<br><br><div style="margin-left: 40px;"> <b>Yes:</b> Continue with step 2.<br/> <b>No:</b> Correct the addresses. Continue with step 4.           </div> |
| 2. | Check the gateway NE identification.   |

Is the gateway NE identification correct?

**Yes:** Continue with step 3.

**No:** Correct the identification. Continue with step 4.

3. Check the Data Communication Network (DCN).

Is the DCN in service?

**Yes:** Continue with step 4.

**No:** Bring the DCN into service.

4. Is the alarm now cleared?

**Yes:** O.K.

**No:** Call Lucent Technologies Technical Support.

#### 6.6.4.7 TL1\_COMM\_DENIED

**Meaning** User login for a TL1 communication session was denied by the NE for all TCP/IP connections opened.

**Abbreviation:** TL1\_COMM\_DENIED

**Severity:** Critical

**Service affecting:** No

The alarm will be cleared when a TL1 communication session between the AEM-NB and the NE has been successfully opened.

**Effects** It is not possible to manage the NE because there is no TL1 communication session available.

**Possible Cause(s)** A user login error is stopping the TL1 communication session establishment process between the AEM-NB and the NE.

**Corrective Actions** Proceed as follows to clear the alarm:

Step	Procedure
1.	Check for correct User Identification (user login), Password and NE target identifier (TID).
2.	Check with the GSI that the four VC in the NE are not busy (RTRV-STATUS TL1 command).

---

# Data Communications Network (DCN) Configuration



---

## Contents

<b>A.1</b>	<b>Overview</b>	<a href="#">A-1</a>
<b>A.2</b>	<b>DCN Introduction</b>	<a href="#">A-1</a>
<b>A.3</b>	<b>Terms Used in this Chapter</b>	<a href="#">A-2</a>
<b>A.4</b>	<b>Network Element Communication Capabilities</b>	<a href="#">A-2</a>
<b>A.5</b>	<b>AEM-NB Communication Capabilities</b>	<a href="#">A-5</a>
<b>A.6</b>	<b>Recommended DCN Configurations</b>	<a href="#">A-5</a>
A.6.1	ROC Over Permanent Leased Lines DCN	<a href="#">A-5</a>
A.6.1.1	Router Configuration	<a href="#">A-6</a>
A.6.1.2	<i>AnyMedia</i> Network Element Configuration	<a href="#">A-7</a>
A.6.1.3	Element Manager Server Configuration	<a href="#">A-8</a>
A.6.1.4	Element Manager Client Configuration	<a href="#">A-8</a>
A.6.1.5	Transport Elements Configuration	<a href="#">A-9</a>
A.6.1.6	Connection Diagram	<a href="#">A-9</a>
A.6.2	Communication with Remote NEs Using Inband ATM PVC	<a href="#">A-10</a>
A.6.2.1	Configuration of the router	<a href="#">A-11</a>
A.6.2.2	Configuration of <i>AnyMedia</i> Network Element	<a href="#">A-12</a>
A.6.2.2.1	Configuration of COMDAC	<a href="#">A-12</a>
A.6.2.2.2	Configuration of AFM	<a href="#">A-12</a>
A.6.2.3	Element Manager Server Configuration	<a href="#">A-12</a>
A.6.2.4	Element Manager Client Configuration	<a href="#">A-12</a>
A.6.2.5	Transport Elements Configuration	<a href="#">A-12</a>
A.6.2.6	Connection Diagram	<a href="#">A-13</a>

---

## Contents



---

## A.1 Overview

This appendix provides you with information about

- DCN introduction,
- General definitions of terms,
- Network Element management communications,
- *AnyMedia* Element Manager management communications,
- Recommended DCN configurations.

---

## A.2 DCN Introduction

### AEM-NB Features

The *AnyMedia*® Access System is designed to provide a full range of narrowband access services like POTS, ISDN and Leased Lines.

The *AnyMedia* Access System Element Manager for Narrowband Services (AEM-NB) will provide the standard management configuration, equipment configuration, fault and testing, performance and security functions capabilities to do service management, monitoring, generate reports and printouts, do backup and restore functions for example to improve the customer's day to day business.

### Communication of AEM-NB and NE

The AEM-NB will communicate with the network elements by using TL1 commands over TCP/IP. The AEM-NB is also prepared in the first release to communicate with other legacy OSs by means of TL1 northbound interfaces. TL1 will be used for request/response and autonomous reports commands and FTP will be used for software and database upload/download operations.

### DCN

The DCN is the communications infrastructure (routers, WAN links, etc.) needed for communication of the AEM-NB with the NEs it manages. This manual refers to AEM-NB Release 1.3 and *AnyMedia* NE Release 1.3. For this releases many DCN configurations and protocol profiles can be used according to the network

operators needs and scenarios. Two sample DCN scenarios are given at the end of this chapter.

## A.3 Terms Used in this Chapter

---

<b>Data Communications Network</b>	The Data Communications Network (DCN) consists of the communication media and the interconnected devices which are used to exchange management information between the AEM-NB, the NEs and other management systems.
<b>Remote Operations Channel</b>	The Remote Operations Channel (ROC) is a bearer channel that conveys management information for a remote system ( <i>AnyMedia</i> NE). The ROC is expected to be used when the system is installed at locations where no Ethernet Local Area Network (LAN) and no separate network (e.g. X.25) exists.
<b>Router</b>	A router is a network layer device that forwards packets from one network to another based on network layer information (OSI layer 3). Data packets are only transferred through the router, if the participant is on another port of the router. The router can keep data traffic certain parts of a local area network (LAN). A router is more powerful than a bridge, it reduces the traffic on a LAN more than a bridge, because the IP address is evaluated for traffic control.
<b>Bridge</b>	A bridge is a network layer device that passes packets between two or more network segments that use the same data link communications protocol (OSI layer 2). The network segments appear as one segment to protocol levels higher than the data link layer. The bridge recognizes with the help of the MAC address which LAN component is on which port of the bridge. Data packets are only transferred over the bridge if the participant is on another port of the bridge. With a bridge data traffic can be kept from certain parts of a LAN.

## A.4 Network Element Communication Capabilities

---

In this section the management communication capabilities of an *AnyMedia* NE R1.3 are described. The *AnyMedia* Access System provides the following management interfaces for operation, administration, maintenance, and provisioning (OAM&P):

- Craft interface terminal (CIT)

The CIT port is a local EIA-232D (former RS-232C) interface. It is located on the faceplate of the CIU card in the *AnyMedia* Access System for 30 channel market. A PC-based Graphical System Interface (GSI-NB) can be connected to the CIT port locally. This interface is typically used during initial installation and other maintenance related activities.

This interface can also be used to remotely manage the NE using the GSI-NB ((e.g. POTS dial-up via modem), PPP is implemented on top of the CIT port as to allow this remote management. The protocol profile in the NE for this scenario is shown in Figure A-1.

---

File Transfer Protocol	TL1 over TCP
TCP at layer 4	TCP at layer 4
IP at layer 3	IP at layer 3
PPP	PPP
RS232	RS232

**Figure A-1** *AnyMedia* Remote Access to CIT Port Protocol Profiles

■ External system LAN interface

LAN interface is available via a backplane connector on the *AnyMedia* Access System shelf. It provides access to an IEEE 802.3 compliant LAN through a 10BaseT connection. All communications through this interface occur over the transmission control protocol/internet protocol (TCP/IP) to the GSI-NB or element manager (AEM-NB). The protocol profile in the NE for this scenario is shown in Figure A-2. For *AnyMedia* NE release 1.7 it will be an IAO LAN (also supporting an OSI protocol stack).

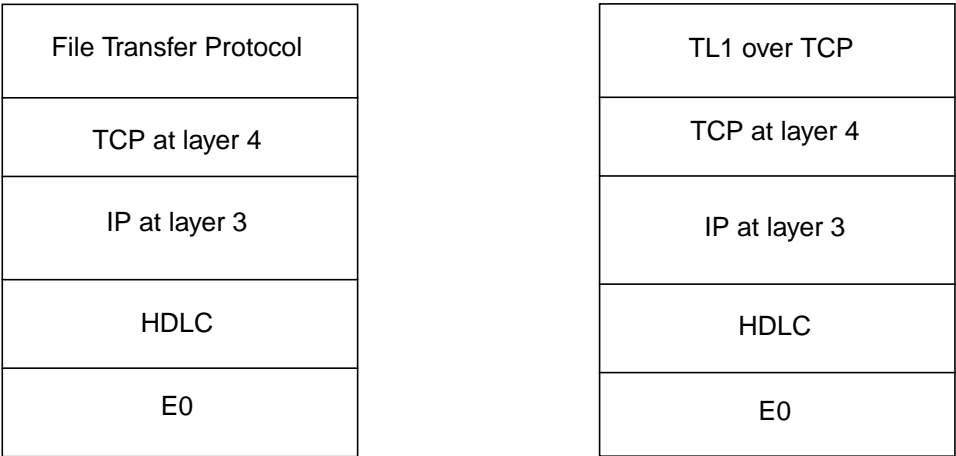
---

File Transfer Protocol	TL1 over TCP
TCP at layer 4	TCP at layer 4
IP at layer 3	IP at layer 3
MAC & LLC-1 at layer 2	MAC & LLC-1 at layer 2
10BaseT at layer 1	10BaseT at layer 1

**Figure A-2** *AnyMedia* External LAN Interface Profiles

■ Remote Operations Channel (ROC)

ROC is a 64 kbps timeslot within the payload of a E1 link bound to a feeder of the *AnyMedia* NE. The *AnyMedia* Access System provides access for a remotely located OS if it communicates via TCP. The protocol profile in the NE for this scenario is shown in Figure A-1. This alternative can be used if no local Ethernet LAN is available or the outside plant (OSP) environment is too severe for a router. It does not need a separate DCN, then it can be a cheaper solution. The protocol profile in the NE for this scenario is shown in Figure A-3.



**Figure A-3    *AnyMedia* Remote Operations Channel (ROC) Protocol Profiles**

For establishing communication between the AEM-NB and the NE, the NE must be minimally configured with its LAN, ROC or CIT parameters as applicable. This option is the only available, as the *AnyMedia* Access System does not support remote boot and remote TCP/IP configuration. The GSI-NB can be used to provide this initial configuration of the NE using the CIT port.



## A.5 AEM-NB Communication Capabilities

The AEM-NB uses for communicating management data an external system LAN interface. The protocol profile in the AEM-NB for this scenario is shown in Figure A-4.

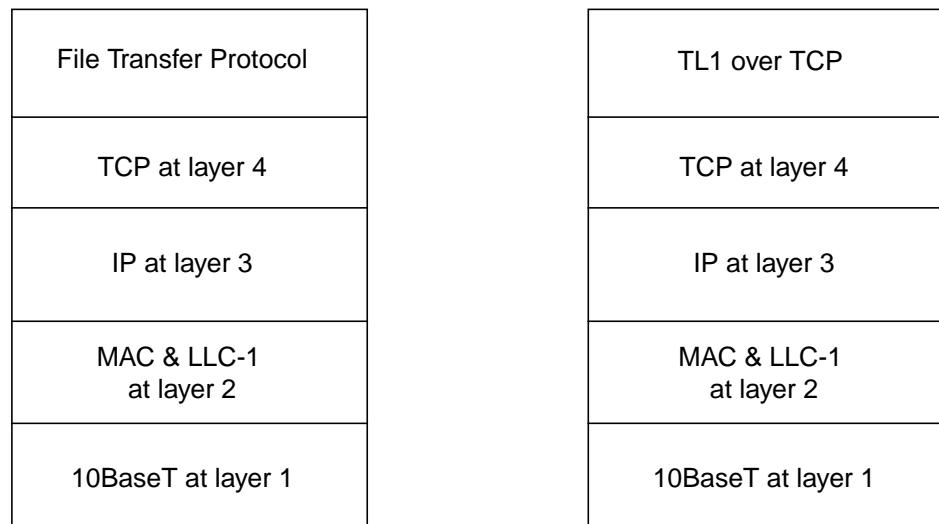


Figure A-4 AEM-NB Protocol Profiles

## A.6 Recommended DCN Configurations

If a data network is not yet available between the central site where the AEM-NB is located and the remote site where the NEs are located, the following two configurations are recommended:

- ROC over permanent leased lines DCN (cf. Chapter A.6.1, page A-5)
- Communication with remote NEs using inband ATM PVC (Chapter A.6.2, page A-10).

### A.6.1 ROC Over Permanent Leased Lines DCN

The assumptions for this configuration are:

- The LAN-based V5DLC AEM-NB is located in the central office.
- The V5DLCs NEs are located in remote locations.

- The OAM&P information (mapped in the 64 kbit/s ROCs) is transported from the AEM-NB in the central office to the remote locations using Permanent Leased Lines (PLLs) which are carried via:
  - SDH equipment in ring or point to point structure. Then a digital cross connect system (e.g. DACS-II) is available in the central office, it extracts the ROCs from each 2 Mbit/s link and put up to 30 ROCs to one 2 Mbit/s link.
  - PDH equipment in point to point structure. Then a digital cross connect system (e.g. DACS-II) is available in the central office, it extracts the ROCs from each 2 Mbit/s link and put up to 30 ROCs to one 2 Mbit/s link.
  - Using existing data communication network (leased line network). Then a leased line service node is available in the central office, it extracts the 64 kbit/s ROCs from each 2 Mbit/s link and concentrates up to 30x64 kbit/s ROCs into a single 2 Mbit/s link to the router (channelized E1 I/F).
- The PLLs will be originated at the AEM-NB side by means of routers and DACS equipment and will be terminated at the COMDAC of the NE which extracts the ROC and its associated management information.
- The router at the AEM-NB side will have to make a translation between E0/HDLC/IP/TCP and the AEM-NB protocol stack 10BaseT/MAC&LLC1/IP/TCP. The AEM-NB side router configuration will have channelized E1 interfaces. The Router/Bridge could be delivered by Lucent Technologies.
- One remote operation channel is used per V5DLC (64 kbit/s ROC carried on a 2 Mbit/s LL I/F).
- In this scenario a feeder is used in every network element to establish PLLs (instead of using it for V5 links), then if the only information which is carried over the PLL feeder is ROC the bandwidth of the transport network is wasted and a new cable is needed to be inserted in this feeder. If one feeder of the NE already supports other customer LLs no waste is made.
- For layer 2 HDLC Protocol is used between V5DLC and the router.
- For up to 30 V5DLC connected to the LE, a single E1 interface for the router/bridge is sufficient.

### A.6.1.1 Router Configuration

The minimal requirements for the router/bridge for supporting this scenario are:

- Minimal WAN interface requirements

The router/bridge must have one or more channelized 2 Mbit/s E1 interfaces (ITU G.703/G.704). Both, the symmetrical 120 ohms resistive (balanced) or the coaxial 75 ohms (unbalanced) resistive versions of the E1 interface should be supported depending on the customer needs. An IP address may be assigned to each time-slot or channel group. HDLC framing needs to be supported at the layer 2 of every slot inside the channelized E1 interface.

- Minimal LAN interface requirements

The router must have one or two (for cascading purpose) Ethernet (IEEE 802.3) 10Base T ports. In case of two LAN ports, LAN-to-LAN routing should be supported.

Provisioning needs for the router/bridge are the following:

- E1 interface functionality (line code, framing type etc.)
- Time-slot mapping (each needed serial interface related to one ROC will be a channel group mapped on a time slot of the channelized E1)
- Protocols and encapsulations
- IP-addresses for IP routing (routing tables)
- Ethernet media.

The initial provisioning of a router/bridge is typically performed by a VT100/ANSI terminal, connected to a RS-232C port. When the IP-address of the router is provisioned, the router may be configured via LAN (TELNET, SNMP) but this depends on the router/bridge being used.

#### A.6.1.2 **AnyMedia Network Element Configuration**

The ROC is the management interface used to access the NE. The initial provisioning has to be done via pre-provisioning (factory settings) or a local GSI-NB (LAN or RS-232C) because the LL interface, carrying the remote operations channel, must be in-service to get remote access to the NE via remote operations channel (ROC). To enable the use of 64 kbit/s bearer channels for remote operations, the following provisioning needs for the V5DLC (30 channel market NE) are required:

- Create a ROC line (virtual port), which can be addressed as remote LAN interface (same IP-address as the local LAN interface on the V5DLC (*ent-roc TL1 command*)).
- Routing of physical LL bearer channel, assigned to the virtual port to the serial communication channel (SCC) of the microcontroller.
- Create a leased line link entity (*ent-lll TL1 command*).
- create a cross connection between the ROC line entity and a 64 kbit/s timeslot of leased line link (*ent-crs-llts TL1 command*).
- Bring ROC channel into service.

On the 30 channel *AnyMedia* NE we must configure the ROC over the NON-V.5 PLL service, and the IP characteristics of the NE. We use TL1 commands to configure the NE by means of the GSI-NB craft terminal, the TL1 commands related to this scenario are listed below. Note that the default router address of the NE must be set to 224.0.0.2 (universal router's multicast address) so that the NE points to the router on the other side of the ROC interface.

```
ent-roc::roc-1;
ent-lll::lll-1:::e1-1-1-1;
```

```
ent-crs-1lts::roc-1,1lts-1-16;
set-ip:::::shelf=135.5.78.2,defrouter=224.0.0.2,submask=255.255.255.0
```

Once communications with the Element Manager are established via the ROC, we can execute remote operations on the NE as if we are connected via the LAN. We can also use either the GSI-NB or a standard windows FTP/TELNET.

### A.6.1.3 Element Manager Server Configuration

<b>Server IP Parameters</b>	<p>The server on which the AEM-NB application resides must have its IP parameters configured:</p> <ul style="list-style-type: none"> <li>■ IP address (e.g. 135.88.20.234)</li> <li>■ subnet mask (e.g. 255.255.240.0)</li> <li>■ default router (e.g. 135.88.17.1).</li> </ul>
<b>Configuration</b>	<p>In the AEM-NB the following parameters have to be configured to be able to communicate with the NEs.</p> <ul style="list-style-type: none"> <li>■ TCP/IP configuration related to NEs <ul style="list-style-type: none"> <li>— For every NE the AEM-NB wants to communicate with, its IP address (e.g. 135.88.4.2) must be introduced in the AEM-NB (provisionable via AEM-NB GUI).</li> <li>— The ports to be used in the NE needs to be stored in the AEM-NB (e.g., for TL1 over TELNET communication the ports to be used are in the order: 11002, 11004, 11006 and 11008; for FTP communication the port number 20 for FTP data transmissions and the port number 21 for FTP control communication).</li> </ul> </li> <li>■ Association configuration related to NEs <ul style="list-style-type: none"> <li>— For every NE with which the AEM-NB has to communicate, the NEs Target Identifier (TID) must be known by the AEM-NB (provisionable via AEM-NB GUI).</li> <li>— For every NE with which the AEM-NB wants to communicate, the LOGIN information related to that NE must be introduced in the AEM-NB (provisionable via AEM-NB GUI).</li> <li>— For every NE the AEM-NB wants to communicate with, the PASSWORD information related to that NE must be known by the AEM-NB (provisionable via AEM-NB GUI).</li> </ul> </li> </ul>

### A.6.1.4 Element Manager Client Configuration

<b>Client IP Parameters</b>	<p>The workstation with the AEM-NB client has the following IP parameters configured. Note that if the client is located at the same machine as the server these parameters are already configured.</p> <ul style="list-style-type: none"> <li>■ IP address (e.g. 135.88.20.230)</li> <li>■ subnet mask (e.g. 255.255.240.0)</li> </ul>
-----------------------------	---

- default router (e.g. 135.88.17.1).

**AEM-NB Preferences File**

In the preferences file of the AEM-NB client the following information must be stored to be able to access the AEM-NB server (this file has to be created before starting the AEM-NB client GUI):

- The AEM-NB server IP address (e.g. 135.88.20.234)
- The LOGIN for accessing the AEM-NB server (encrypted)
- The PASSWORD for accessing the AEM-NB server (encrypted).

**A.6.1.5 Transport Elements Configuration**

If transport is achieved by means of SDH equipment in ring or point to point structure, then:

- The paths (i.e. VC-12 paths) used for transporting the E1 links need to be provisioned.
- The digital cross connect system which extracts the ROCs from each 2 Mbit/s link and put up to 30 ROCs to one 2 Mbit/s link need to be configured. For up to seven remote V5DLC the TMN-252 SCX can be used.

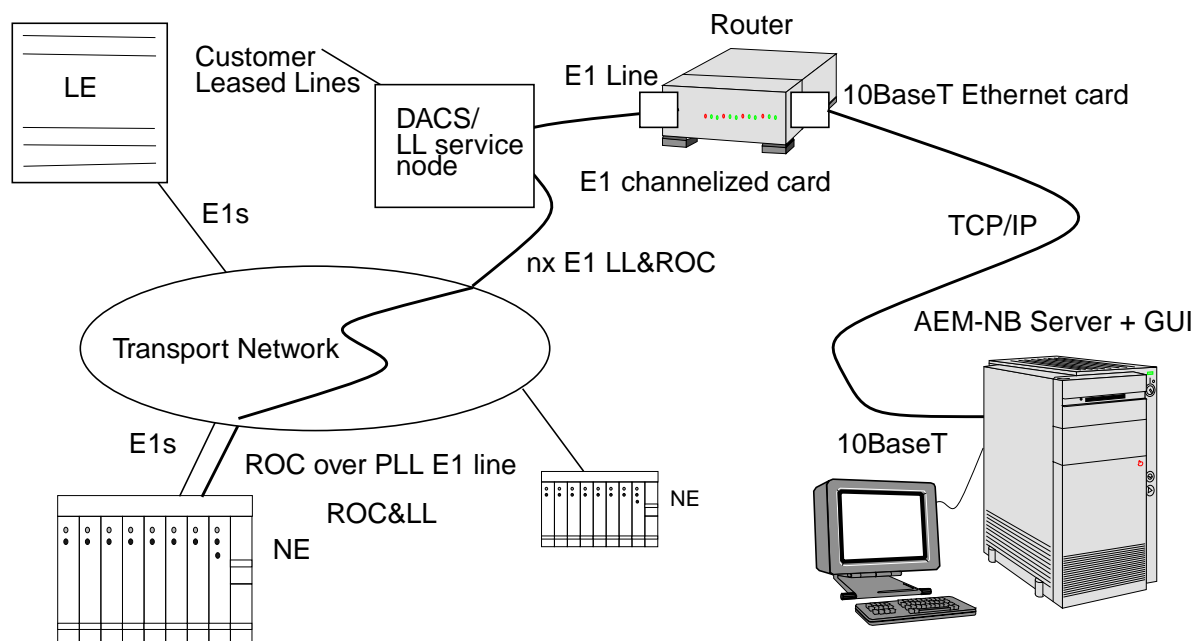
If transport is achieved by means of PDH equipment in point to point structure, then:

- The E1 paths used for transporting the ROCs through the PDH network need to be provisioned.
- The digital cross connect system which extracts the ROCs from each 2 Mbit/s link and put up to 30 ROCs to one 2 Mbit/s link need to be configured. For up to 7 remote V5DLCs the TMN-252 SCX can be used.

If transport is achieved by means of leased line networks. Then a leased line service needs to be provisioned.

**A.6.1.6 Connection Diagram**

For testing purposes, the E1 interface of the E1 router may be either directly connected to the E1 feeder of the NE or may be connected to this feeder using an intermediate transport network and/or a crossconnect equipment.



**Figure A-5 Configuration of 30 channel Permanent Leased Line Access to ROC**

### A.6.2 Communication with Remote NEs Using Inband ATM PVC

The assumptions for this configuration are:

- There are broadband and narrowband access technologies collocated in the same NE. Narrowband access is oriented to telephony applications and is based on V5 interfaces, broadband access is oriented to data applications and is based on Asynchronous Transfer Mode (ATM) over Asymmetrical Digital Subscriber Line (ADSL) access. The broadband access consists of ADSL application packs and Access Feeder Multiplexer (AFM) control cards which make the switching between ADSL access traffic and ATM networks using E3 interfaces (30 channel market).
- There is an ATM network between Central Office and remote *AnyMedia* NEs.
- In this scenario ATM Permanent Virtual Circuits (PVCs) are used to communicate narrowband (TL1/FTP over TCP based) and broadband (SNMP over UDP and FTP over TCP based) management traffic between AEM-NB/BB Element Managers and *AnyMedia* NEs.
- One ATM PVC will be used for every NE to be managed, this ATM PVC carries IP packets related to both COMDAC and AFM management information.
- ATM PVCs carrying management information related to one NE are originated in a LAN environment where AEM-NB and AEM-BB are located.

- A DCN device is needed at the Central Office to make the translation between 10BaseT/MAC&LLC1/IP and E3/ATM PVC/AAL5/802.2 LLC/802.2 SNAP/IP interface to the ATM network. The LLC encapsulation method to be supported by that device is that described in RFC 1483 [7], i.e. this method allows multiplexing multiple protocols over a single ATM virtual circuit. Further, this method carries connectionless network traffic over the ATM network. Note that this functionality (if available) can also be performed by the ATM switch connected by means of a LAN connection with the Central Office (e.g. CBX-500), in these cases there is no need of a separate ATM router at the CO.
- ATM PVC which carries IP management information is carried over an ATM network and finally they are inserted in a related NE by means of E3 data ports, IP packets contained in the ATM PVC are extracted in the Broadband AFM card which also support RFC 1483.
- Part of these IP packets (those with IP address of AFM) which carry BB management information are terminated in AFM.
- Part of these IP packets (those with IP address of COMDAC) which carry NB management information are forwarded to AFM LAN port which is joined to COMDAC LAN port (located on the top front panel of the *AnyMedia* shelf), these IP packets will be terminated in the COMDAC.

### A.6.2.1 Configuration of the router

The router at Central Office need to be configured. The minimal requirements for the router for supporting this scenario are:

- Minimal WAN interface requirements  
The router must have one or more ATM E3s interfaces with the ATM network (or any other physical interface, e.g. E1 depending on the edge ATM switch to interface with). It is in charge of mediating from 10BaseT/MAC&LLC1/IP to E3/ATM PVC/AAL5/802.2 LLC/802.2 SNAP/IP. The logical WAN interface should be compatible with that of the connected ATM switch (e.g. Support of UNI 3.1 & 4.0 ATM cell switching). This router must support RFC 1483 (multiprotocol over ATM encapsulation) since AFM supports it.
- Minimal LAN interface requirements  
The router must have one or two (for cascading purpose) Ethernet (IEEE 802.3) 10BaseT/100BaseT ports. In case of two LAN ports, LAN-to-LAN routing should be supported.

The configuration tasks to be performed on router are:

- Configure ATM E3 Interface
- Configure LAN interface
- Configure ATM PVCs inside that physical interface and assign to them IP addresses
- Create routing tables for both AFM and COMDAC (e.g. those IP packets to be sent to AFM or IP addresses should be routed to the related PVC).

## **A.6.2.2 Configuration of *AnyMedia* Network Element**

### **A.6.2.2.1 Configuration of COMDAC**

On the *AnyMedia* Narrowband part of NE we must configure the Local LAN port. The initial provisioning has to be done via pre-provisioning (factory settings) or a local GSI-NB (RS-232C). To do so we must configure the Narrowband LAN port IP address, the default router address (address of AFM LAN port) and the subnet mask of the NE local LAN port. We use TL1 commands to configure the NE as it is shown in the next example.

```
set-ip::::::shelf=135.88.4.2,defrouter=135.88.17.1,submask=255.255.240.0
```

### **A.6.2.2.2 Configuration of AFM**

On the AFM we must configure the in-band ATM Permanent Virtual Circuit (PVC) which is carrying NB and BB management information. This ATM PVC will be terminated at AFM and IP packets contained in it will be extracted. For this PVC VPI should be 0 and VCI greater than 31. ATM PVCs may be provisioned in AFM by means of GSI-BB via local CIT altogether with AFM IP addresses (one for E3 interface and another one for LAN port). IP, Net Mask and Gateway addresses for AFM must be provisioned.

On the AFM we must configure a routing table (i.e. so that IP packets related to COMDAC are forwarded to the AFM LAN port and IP packets related to AFM are terminated at AFM)

We must join AFM LAN port with COMDAC LAN port located on top front panel of the FAST shelf by means of a Ethernet cross over cable.

## **A.6.2.3 Element Manager Server Configuration**

The element manager server configuration is the same as described in Chapter A.6.1.3, page A-8.

## **A.6.2.4 Element Manager Client Configuration**

The element manager client configuration is the same as described in Chapter A.6.1.4, page A-8.

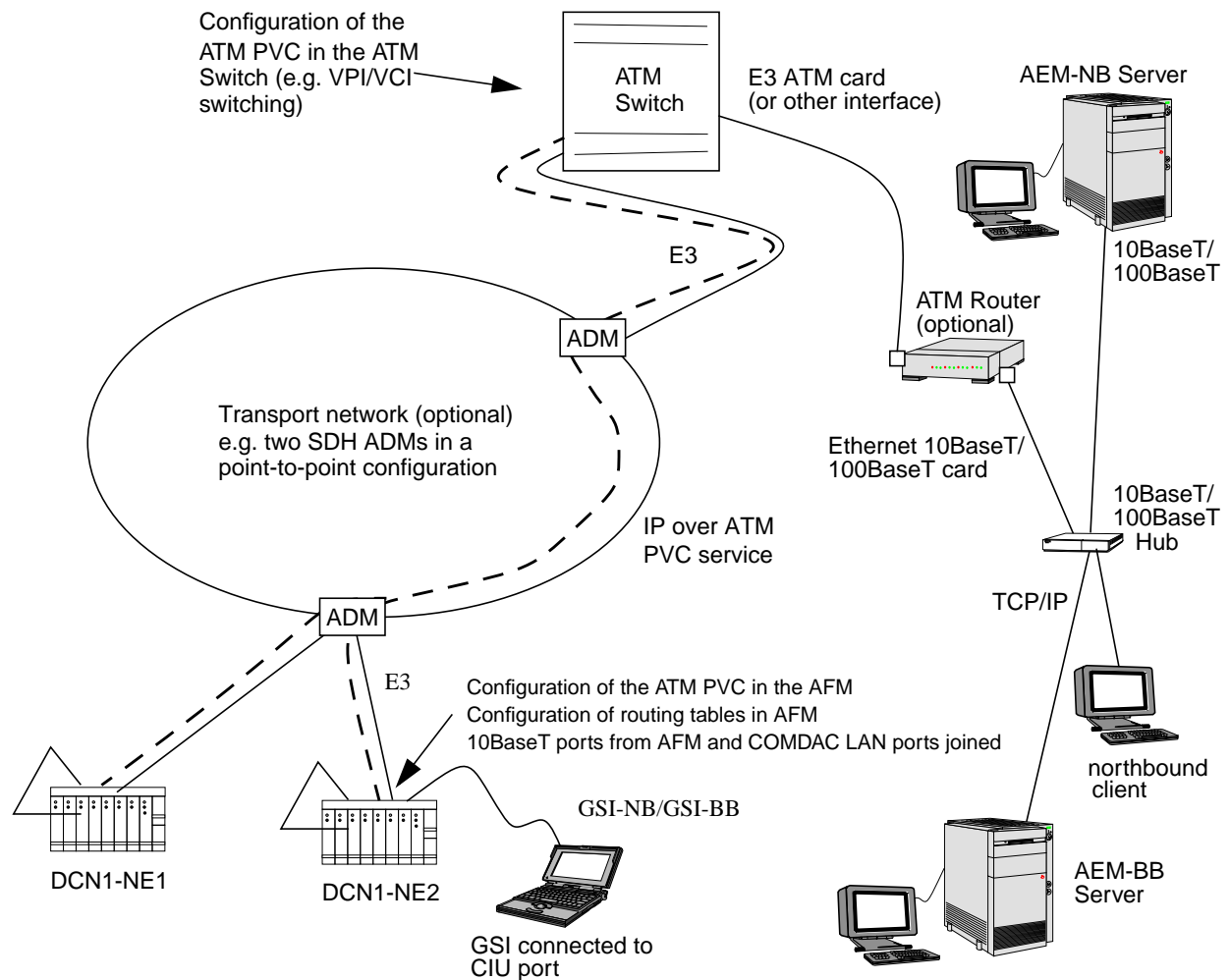
## **A.6.2.5 Transport Elements Configuration**

The ATM switches which will transport the ATM PVCs carrying the IP management traffic need to be provisioned, i.e a table must be provisioned in these switches saying that the cells from a specific VPI/VCI are related to a VPI/VCI pair in another interface. The ATM router and *AnyMedia* NEs must be attached to the ATM network by using E3 links (for the ATM router other links may also be used, e.g. E1/STM-1, etc.). If the switch supports directly rfc1483 a direct LAN connection between the switch and the CO LAN environment must be provisioned, in this case there is no need of ATM router at the CO side.



If SDH ADMs are used the paths which carry the ATM information need to be provisioned.

### A.6.2.6 Connection Diagram



**Figure A-6 Communication with Remote NEs using in-band ATM PVC**



---

# System Variables and Configuration Parameters

# B

---

## Contents

<b>B.1</b>	<b>Overview</b>	<a href="#">B-1</a>
<b>B.2</b>	<b>System Variables</b>	<a href="#">B-1</a>
<b>B.3</b>	<b>Configuration Parameters</b>	<a href="#">B-2</a>
B.3.1	<i>AnyMedia</i> Server Configuration Parameters	<a href="#">B-2</a>
B.3.2	<i>AnyMedia</i> Client GUI Configuration Variables	<a href="#">B-4</a>

---

## Contents

---

# System Variables and Configuration Parameters

# B

---

## B.1 Overview

This appendix provides you with information about

- System variables and
- Configuration parameters.

---

## B.2 System Variables

The values of some system variables are specified in the file **AnyMediaNBEM.cfg** which is located in the directory **\$ANYMEDIAPATH/cfg/**. The system variables can be changed by editing their values in this file with a text editor. The changes take effect after the system is restarted.

The following table shows selected variable names, their meaning and default values. The locations of the directories are relative to the main installation directory of the AEM-NB.

**Table 2-1 System Variables and their Default Values**

System Property	Variable Name	Default Value
Location of alarm database	AM.databaseLocation	<b>AM/db</b>
Location of configuration management database	CM.databaseLocation	<b>CM/db</b>
Location of NE management database	NEM.databaseLocation	<b>NEM/db</b>
Location of security database	OAM.security.databaseLocation	<b>Security/db</b>
Location of Non-volatile Data Storage (NVDS)	CM.directoryNVDS	<b>CM/nefiles/NVDS</b>

**Table 2-1 System Variables and their Default Values**

System Property	Variable Name	Default Value
Location of log files	OAM.log.directoryCurrentLogs	log
Minimum number of days (incl. current day) in the log	OAM.log.minimumDaysKept	7
Maximum size of all logged data	OAM.log.maximumTotalLogSize	15
Stop OrbixMT (3rd party software) when the AEM-NB goes down	Gen.3rdParty.mgmtOrbixMT	true
Stop OrbixNames (3rd party software) when the AEM-NB goes down	Gen.3rdParty.mgmtOrbixNames	true
Stop OrbixTalk (3rd party software) when the AEM-NB goes down	Gen.3rdParty.mgmtOrbixTalk	true
Stop ObjectStore (3rd party software) when the AEM-NB goes down	Gen.3rdParty.mgmtObjectStore	true

## B.3 Configuration Parameters

This chapter provides information about all the configuration parameters that are used with AEM-NB R1.3, as follows:

- An alphabetical list of all configuration parameters that are used with AEM-NB R1.3.
- Detailed information about each parameter.

These configuration parameters are distributed in three configuration files, as follows:


- **AnyMediaNBEMR1.3.cfg** for variables used by the *AnyMedia* servers.
- **AnyMedia.ini** and **SystemPreferences.ini** for variables used by the GUI.

Only the configuration parameters the *AnyMedia* administrator can modify are explained in this chapter -modify these configuration variables with caution as they may adversely affect the correct operation of the application-. To modify the other configuration parameters stored in the configuration files, please contact with Lucient Technologies TCL.

### B.3.1 *AnyMedia* Server Configuration Parameters

The following table provide an alphabetical list of the configuration parameters for *AnyMedia* servers.


**Table 2-2 AnyMediaNBEM.cfg File**

	Name	Description
<b>Configuration Management Settings</b>	CM.directoryNVDS	NVDS files location. This files store information in such a way as to survive indefinite periods of total power failure. The current values for all provisionable parameters are store in the NVDS directory and hence are the parameter values that will be used on subsequent NE power-up.  Default value: CM/nefiles/NVDS.
	 <b>NOTE:</b> All paths showed as default value are relative to the <i>AnyMedia</i> installation path.	
<b>OAM Settings</b>	CM.directoryNVPS	NVPS files location. It keeps software program data. It resides in the NE <COMDAC>  Default value: CM/nefiles/NVPS.
	OAM.backup.archiveDirectory	default path or device -like a Tape unit- where the <i>AnyMedia</i> archives will be placed.  Default value: archives.
	OAM.backup.backupDirectory	default path or device -like a Tape unit- where the <i>AnyMedia</i> backups will be placed.  Default value: backups.
	OAM.backup.backupLogDirectory	default path where the backup's logs will be placed.  Default value: tmp.
	OAM.backup.numberOfLogFiles	maximum number of backup's log files. Range of values: 1 to 10 Default value: 10.
	OAM.log.directoryCurrentLogs	default path where the restored <i>AnyMedia</i> logs will be placed from a previous archive.  Default value: log.
	OAM.log.directoryRestoredLogs	default path where the <i>AnyMedia</i> restored logs will be placed.  Default value: restored.
	OAM.log.maximumTotalLogSize	maximum size in kilobytes for all <i>AnyMedia</i> log files.  Default value: 15000.
	OAM.log.minimumDaysKept	log's latency period in days.  Default value: 7.

### B.3.2 *AnyMedia* Client GUI Configuration Variables

The following table provides an alphabetical list of the configuration parameters for *AnyMedia* GUI.

**Table 2-3    SystemPreferences.ini Configuration File**

	Name	Description
Site Settings	SITE	the city or the location where the Element Manager is working. This value is used for printing purposes.
	LOC_TIME_ZONE	code for the representation of names of time zones.  Range of values: <b>GMT</b> (Greenwich Mean Time), <b>ECT</b> (European Central Time), ...  Default value: defined at installation time.
User View Settings	USERVIEW	default view in User Administration window.  Range of values: users, usergroups, domains or objects.  Default value: users.
Alarm Viewer Settings	ALM_VIEW	default view.  Range of values: view1, view2, view3 or view4.  Default value: view1.
	ALM_FILTER	default alarm filter.  Range of values: Last24h, CritRaised, Raised, Host, CritNotCleared, OwnedAck, Clear, AllAck or All.  Default value: Last24h.
 <b>NOTE:</b> The following parameters are used for alarms notification purposes. The notification can be either a visual effect -in the <i>AnyMedia</i> GUI main window the flag icon changes to up state and the count of notified alarms is increased- or/and audio effect -a beep sound is generated (only on the server).		
	VISUAL_CRITICAL_ALARM_SEV	enable-disable visual notification of critical severity alarms.  Range of values: true (to enable) or false (to disable).  Default value: true.



**Broad-Band Application Settings**

<b>Name</b>	<b>Description</b>
VISUAL_MAJOR_ALARM_SEV	enable-disable visual notification of major severity alarms.  Range of values: true (to enable) or false (to disable).  Default value: false.
VISUAL_MINOR_ALARM_SEV	enable-disable visual notification of minor severity alarms.  Range of values: true (to enable) or false (to disable).  Default value: false.
VISUAL_INFO_ALARM_SEV	enable-disable visual notification of information severity alarms.  Range of values: true (to enable) or false (to disable).  Default value: false.
AUDI_CRITICAL_ALARM_SEV	enable-disable audio notification of critical severity alarms.  Range of values: true (to enable) or false (to disable).  Default value: true.
AUDI_MAJOR_ALARM_SEV	enable-disable audio notification of major severity alarms.  Range of values: true (to enable) or false (to disable).  Default value: false.
AUDI_MINOR_ALARM_SEV	enable-disable audio notification of minor severity alarms.  Range of values: true (to enable) or false (to disable).  Default value: false.
AUDI_INFO_ALARM_SEV	enable-disable audio notification of information severity alarms.  Range of values: true (to enable) or false (to disable).  Default value: false.
BROAD_BAND_URL	the URL where the Broad Band application is located.  Default value: defined at installation time.

<b>Cut-Through Settings</b>	Name	Description
	LOGTELNET	login to connect to AEM-NB server for Cut-Through purposes. Default value: defined at installation time.
	PASSTELNET	password to connect to AEM-NB server for CutThrough purposes. Default value: defined at installation time.
<b>Help Settings</b>	SERVER	server host where the AEM-NB application is running. Default value: defined at installation time.
	HELP_URL	the URL where the help files are located.

**Table 2-4 AnyMedia.ini Configuration File**

Name	Description
LV_READLINES	line number of server log messages read in Log Viewer. Range of values: 1 to 50. Default value: 50.

---

## Contents

<b>C.1</b>	<b>Overview</b>	<a href="#">C-1</a>
<b>C.2</b>	<b>Northbound Interface Basics</b>	<a href="#">C-1</a>
C.2.1	Northbound Interface Description	<a href="#">C-1</a>
<b>C.3</b>	<b>Northbound Interface Specific TL1 Messages</b>	<a href="#">C-3</a>
C.3.1	REPT ALM (Report Alarm)	<a href="#">C-4</a>
C.3.1.1	Purpose	<a href="#">C-4</a>
C.3.1.2	Output Format	<a href="#">C-4</a>
C.3.1.3	Output Format Parameters	<a href="#">C-4</a>
C.3.2	RTRV-ALM (Retrieve-Alarms)	<a href="#">C-9</a>
C.3.2.1	Purpose	<a href="#">C-9</a>
C.3.2.2	Input Format	<a href="#">C-9</a>
C.3.2.3	Input Format Parameters	<a href="#">C-9</a>
C.3.2.4	Output Format	<a href="#">C-10</a>
C.3.2.5	Output Format Parameters	<a href="#">C-10</a>
C.3.2.6	Generic Error Responses	<a href="#">C-14</a>
C.3.3	RTRV-ALM-ENV (Retrieve-Alarm-Environment)	<a href="#">C-15</a>
C.3.3.1	Purpose	<a href="#">C-15</a>
C.3.3.2	Input Format	<a href="#">C-15</a>
C.3.3.3	Input Format Parameters	<a href="#">C-15</a>
C.3.3.4	Output Format	<a href="#">C-16</a>
C.3.3.5	Output Format Parameters	<a href="#">C-16</a>
C.3.3.6	Generic Error Responses	<a href="#">C-18</a>

---

## Contents

## C.1 Overview

---

This appendix provides you with information about the

- Northbound interface basics and
- Northbound interface specific TL1 messages.

## C.2 Northbound Interface Basics

---

### C.2.1 Northbound Interface Description

---

#### General

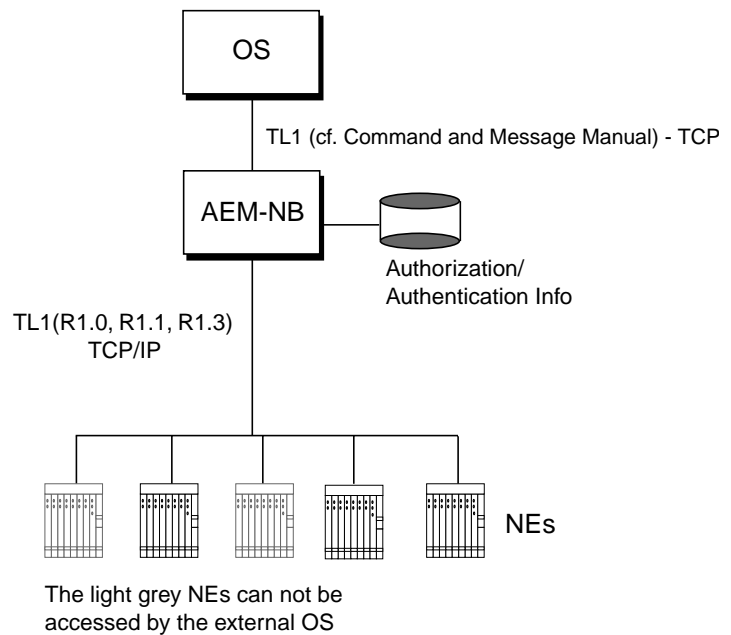
The *AnyMedia*® Access System Element Manager for Narrowband Services (AEM-NB) Release 1.3 offers to any external OS a straight TL1 connection with the set of NEs in the OS's network. Using this link, any external OS with access rights to open a northbound interface session, can configure, test or monitor a set of NEs using a TL1 interface and can receive the responses to the TL1 commands and the autonomous outputs which are generated by the NE (depending on the northbound interface application type selected).

#### Two Types of Northbound Interfaces

The AEM-NB provides two different types of northbound interface applications:

- General northbound interface  
all types of autonomous messages received from the NE are sent to the OS. None NE autonomous messages will be inhibited.
- Alarm only northbound interface  
only alarm and environment alarm autonomous message received from the NE are sent to the OS, the AEM-NB will inhibit the rest of NE autonomous messages (database changes, events, etc...).

<b>Configure Terminal for Session</b>	Before the telnet session for the northbound interface is opened the <b>TERM</b> variable must be set correctly. Set the <b>TERM</b> variable either to <b>dtterm</b> , <b>xterm</b> or <b>vt100</b> .
<b>Restrictions with Multiple Sessions</b>	While a northbound interface session is already open another session of a different type must not be opened for the same NE.
<b>Avoid Interference with other EM</b>	When a northbound interface session is opened it is recommendable to send the message <b>ALW-MSG::vc-all::: ,ALL;</b> to avoid that changes in the configuration of the NE introduced by another manager could interfere with our application.
<b>Start Northbound Interface Session</b>	<p>To start a northbound interface session, the OS must open a TCP/IP connection with the AnyMedia Element Manager. Then a TL1 interface, see <i>Command and Message Manual</i>, is used.</p> <p>Firstly, the OS is authenticated and authorized via the ACT-USER message. The AEM-NB opens a dedicated TL1 virtual circuit with every NE included in the domain of the external OS. When the connections are open, any TL1 command typed by the OS operator, will be sent, to the proper NE, and the responses to these commands, as well as all the available autonomous output messages (AO) will be routed to the proper OS.</p>
<b>Close Northbound Interface Session</b>	To close the northbound interface session, the external OS uses the CANC-USER TL1 message. When this message reaches the AEM-NB, it logs-out the external OS, closes all the TCP/IP connections which are involved in this northbound interface session (both sides, northbound to the OS, and southbound to the NEs managed by the OS) and logs the end of the northbound interface link.
<b>Maintaining Authentication Information</b>	The OS will be authenticated and authorized by the AEM-NB not by the NE. Using this mechanism, the OS will only have to send one ACT-USER TL1 message, which will be spawned by the AEM-NB to all the NEs in the network managed by the OS. To do that, the AEM-NB will have to maintain some information, e.g. the TIDs and IP addresses of all the NEs managed by the OS, and a UID - PID pair to open a virtual circuit on each NE. The AEM-NB operator will be provided with the required set of script tools to maintain this information easily.
<b>Close Virtual Circuits with NEs</b>	In the same way, only one CANC-USER message, sent by the OS to the AEM-NB, will be enough to close all the virtual circuits with the NEs, and the northbound interface session.
<b>Routing of TL1 Messages</b>	For the routing of the TL1 messages, the NEs TID is used, and from every NE configuration table, the corresponding IP address is determinated. Incoming messages that have no TID (field empty), are sent to all connected NEs.
<b>Messages from NEs</b>	In case the OS will send a TL1 request message, the OS has to support as many completion responses as NEs are connected. Messages coming from the NEs (responses and autonomous output), are queued until they are complete (i.e. received) and then sent to the northbound OS. There are no guarantees about the order in which responses are sent to the OS.



**Figure C-1 Northbound Interface**

The number of concurrent northbound interface sessions supported by a single NE will depend on the number of available virtual circuits on the NE.

The AEM-NB will provide the independence of the northbound interface sessions and the AEM-NB GUI interface, so an operator using the AEM-NB GUI, will not get to know whether a northbound interface session is running or not.

### C.3 Northbound Interface Specific TL1 Messages

Some TL1 messages feature more parameters when invoked via AEM-NB. These TL1 messages are described in this section, namely

- REPT ALM (Report Alarm)
- RTRV-ALM (Retrieve-Alarms)
- RTRV-ALM-ENV (Retrieve-Alarm-Environment).

### C.3.1 REPT ALM (Report Alarm)

#### C.3.1.1 Purpose

A REPT ALM (Report Alarm) message is generated autonomously by the NE to report the occurrence of an equipment, facility, or system alarm condition to the OS/AEM-NB and CIT. An alarm condition reported via the REPT ALM message has a corresponding REPT ALM clearance message that is generated when the alarm condition clears.

Abortable	No
Privilege Code	Reports Only
GSI Confirmation Required	No
File Transfer	No
Related Autonomous Message	None

#### C.3.1.2 Output Format

If the command request completes successfully, the following normal completion response is returned:

```
sid date time
AC atag REPT ALM AIDTYPE

"AID:NTFCNCDE,CONDTYPE,SRVEFF,OCRDAT,OCRTM:CONDDSCR"
;
```

#### C.3.1.3 Output Format Parameters

##### AID Access Identifier

This parameter appears in the Access ID Block

Type	Access ID
Required	Yes

AID is the address of the equipment or facility for which an alarm is being reported.

Expert	English
ap-1-{1-16}	Application Pack
ciu-1	Communication interface unit
comdac-1-{1-2}	COMDAC
drop-1-{1-16}-{1-32}	drop



Expert	English
e1-1-{1-4}-{1-4}	E1 physical port (feeder side)
ioe1-1-{1-4}	E1 circuit pack
iohdlc-1-{1-2}	IOHDLIC Circuit Pack
pwrsrc-1-{a,b}	Power Source
sclk-1	Station Clock
sh-1	Shelf
v5i-{1-16}	v5 interface
v5l-{1-16}	v5 Link
v5ts-{1-16}-{1-31}	v5 Time Slot
{string} <sup>a</sup>	NE TID (Target Identifier)

a only available via AEM-NB

## NTFCNCDE Notification Code

This parameter appears in the Common Block

Type	List
Required	Yes

NTFCNCDE is the alarm level.

Expert	English	Comment
CL	Cleared Alarm	
CR	Critical Alarm	
MJ	Major Alarm	
MN	Minor Alarm	

## CONDTYPE Condition Type

This parameter appears in the Common Block

Type	List
Required	Yes

CONDTYPE is a code denoting the condition type. A message reporting the clearing of an alarm has the same condition type as the one reporting the alarm.

Expert	English	Comment
AIS	Alarm indication signal	
BKUPMEMP	System data memory mismatch	
CABLE	Cable disconnect	
CPYMEMF	Copy program memory failed	
DATASYSCR	Data system failed critical	
DATASYSMJ	Data system failed major	
DATASYSMN	Data system failed minor	
DBCRRPT	Data memory corrupt	
DBMEMTRF	Data memory update abort	
EXT	External failure	
IMPROPRMVL	Improper removal	
INT	Internal hardware failure	
LOF	Loss of frame	
LOS	Loss of signal	
NE_ASSOC_FAILED <sup>a</sup>	Assoc with NE failed	
PACKM	Pack mismatch	
POLL	Not responding to poll	
PRCDERR	Procedural error	
PSTNF	Restart PSTN failed	
PWR	Power fault	
PWROVLD	Power overload	
RAI	Remote alarm indication	
RINGF	Ring source input failed	
SERVGRP	Server group maintenance limit exceeded	
SFTCRRPT	Software program corrupt	
SFTERR	Software version mismatch	
SWFTDWNF	Software download failed	
SYNC	Synchronization input failed	
SYNCOOS	System free running	
T-BERL	BER exceeds threshold	
T-BERLN	BER exceeds threshold near end	

Expert	English	Comment
T-FC-CABLE	Cable suspect exceeds failure count threshold	
T-FC-INT	Internal pack failure exceeds failure count	
UNXPRS	Unexpected reset	

a only available via AEM-NB

## SRVEFF Service Effect

This parameter appears in the Common Block

Type	List
Required	Yes

SRVEFF indicates the effect of the reported alarm on service.

Expert	English	Comment
NSA	Non Service Affecting	
SA	Service Affecting	

## OCRDAT Occurrence Date

This parameter appears in the Common Block

Type	Date
Required	Yes

OCRDAT indicates the date of the condition being reported and has the format YY-MM-DD (year-month-day). 70<=yy<=99 maps to 1970 through 1999 respectively; 00<=yy<=37 maps to 2000 through 2037 respectively.

## OCRTM Occurrence Time

This parameter appears in the Common Block

Type	Time
Required	Yes

OCRTM indicates the time of the condition being reported and has the format HH-MM-SS (hours-minutes-seconds).

**CONDDESCR****Condition Description**

Type	String
Required	Yes
Min # chars	1
Max # chars	68

This is the text description for the reported alarm condition. This information can be found in the Correlations Tables. The 68 characters included a pair of escaped quotes "\".

**AIDTYPE****Access Identifier Type**

Type	List
Required	Yes

MODIFIER is the message modifier to the REPT ALM message.

Expert	English	Comment
COM	Common	
E1	E1	
EQPT	Equipment	

## C.3.2 RTRV-ALM (Retrieve-Alarms)

### C.3.2.1 Purpose

The RTRV-ALM (Retrieve-Alarms) command instructs the system to retrieve: (1) all currently active alarms, (2) currently active equipment alarms, (3) currently active facility alarms, or (4) currently active system level alarms from the system.

### C.3.2.2 Input Format

**RTRV-ALM-[AIDTYPE]:[tid]::[ctag];**

Abortable	Yes
Privilege Code	Reports Only
GSI Confirmation Required	No
File Transfer	No
Related Autonomous Message	None

### C.3.2.3 Input Format Parameters

**tid**

#### Target ID

This parameter appears in the TID Block

<b>Type</b>	<b>String</b>
Required	No
Default Type	Dynamic

Target ID is the name of the system to which the command is addressed.

**ctag**

#### Correlation Tag

This parameter appears in the CTAG Block

<b>Type</b>	<b>String</b>
Required	No
Default Type	Dynamic

This field is used to associate the command message to the response message.

**AIDTYPE****Access Identifier Type**

Type	List
Required	No
Default Type	Fixed
Default	ALL

Access identifier type

Expert	English	Comment
ALL	All	
COM	Common	
E1	E1	
EQPT	Equipment	

**C.3.2.4 Output Format**

If the command request completes successfully, the following normal completion response is returned:

```
sid date time
M ctag COMPLD
```

```
"AID,AIDTYPE:NTFCNCDE,CONDTYPE,SRVEFF,OCRDAT,OCRTM:CONDDESCR"
;
```

**C.3.2.5 Output Format Parameters****AID****Access Identifier**

This parameter appears in the Access ID Block

Type	Access ID
Required	Yes
Default Type	Fixed
Default	It-all

This is the address of the equipment and/or facility for which an alarm condition is being reported. Note: If the Modifier=COM, the Access ID is null.

Expert	English
ap-1-{1-16}	Application Pack
ciu-1	Communication interface unit
comdac-1-{1-2}	COMDAC
drop-1-{1-16}-{1-32}	drop
e1-1-{1-4}-{1-4}	E1 physical port (feeder side)
ioe1-1-{1-4}	E1 circuit pack
iohdlc-1-{1-2}	IOHDLC Circuit Pack
pwrsrc-1-{a,b}	Power Source
sclk-1	Station Clock
sh-1	Shelf
v5i-{1-16}	v5 interface
v5l-{1-16}	v5 Link
v5ts-{1-16}-{1-31}	v5 Time Slot
{string} <sup>a</sup>	NE TID (Target Identifier)

a only available via AEM-NB

## AIDTYPE

### Access Identifier Type

This parameter appears in the Access ID Block

Type	List
Required	Yes

Expert	English	Comment
ALL	All	
COM	Common	
E1	E1	
EQPT	Equipment	

## NTFCNCDE

### Notification Code

This parameter appears in the Common Block

Type	List
Required	Yes

This is notification code associated with a single alarm condition.

Expert	English	Comment
CR	Critical Alarm	
MJ	Major Alarm	
MN	Minor Alarm	

## CONDTYPE Condition Type

This parameter appears in the Common Block .

Type	List
Required	Yes

Expert	English	Comment
AIS	Alarm indication signal	
BKUPMEMP	System data memory mismatch	
CABLE	Cable disconnect	
CPYMEMF	Copy program memory failed	
DATASYSCR	Data system failed critical	
DATASYSMJ	Data system failed major	
DATASYSMN	Data system failed minor	
DBCRRPT	Data memory corrupt	
DBMEMTRF	Data memory update abort	
EXT	External failure	
IMPROPRMVL	Improper removal	
INT	Internal hardware failure	
LOF	Loss of frame	
LOS	Loss of signal	
NE_ASSOC_FAILED <sup>a</sup>	Assoc with NE failed	
PACKM	Pack mismatch	
POLL	Not responding to poll	
PRCDERR	Procedural error	
PSTNF	Restart PSTN failed	
PWR	Power fault	
PWROVLD	Power overload	
RAI	Remote alarm indication	
RINGF	Ring source input failed	



Expert	English	Comment
SERVGRP	Server group maintenance limit exceeded	
SFTCRRPT	Software program corrupt	
SFTERR	Software version mismatch	
SWFTDWNF	Software download failed	
SYNC	Synchronization input failed	
SYNCOOS	System free running	
T-BERL	BER exceeds threshold	
T-BERLN	BER exceeds threshold near end	
T-FC-CABLE	Cable suspect exceeds failure count threshold	
T-FC-INT	Internal pack failure exceeds failure count	
UNXPRS	Unexpected reset	

a only available via AEM-NB

**SRVEFF****Service Effect**

This parameter appears in the Common Block

Type	List
Required	Yes

This indicates the reported alarm condition is service-affecting or non-service affecting.

Expert	English	Comment
NSA	Non Service Affecting	
SA	Service Affecting	

**OCRDAT****Occurrence Date**

This parameter appears in the Common Block

Type	Date
Required	Yes

This indicates the date of the condition being reported and has the format YY-MM-DD (year-month-day). 70<=yy<=99 maps to 1970 through 1999 respectively; 00<=yy<=37 maps to 2000 through 2037 respectively.

**OCRTM****Occurrence Time**

This parameter appears in the Common Block

Type	Time
Required	Yes

This indicates the time of the condition being reported and has the format hours:minutes:seconds.

**CONDESCR****Condition Description**

Type	String
Required	Yes
Min # chars	1
Max # chars	68

This is the text description for the reported alarm condition. This information can be found in the Correlations Tables. The 68 characters included a pair of escaped quotes "\".

**C.3.2.6 Generic Error Responses**

Code	Definition	Reason For Code
CLOS <sup>a</sup>	NE Connection Not Available	Connection with the <NE TID> is not available
IITA	Input, Invalid Target Identifier	TID does not match with SID, has unallowed characters, or string is too long
IICT	Input, Invalid Correlation Tag	Incorrect CTAG
IBNC	Input, Block Not Consistent.	Parameter entered in the wrong block.

<sup>a</sup> only available via AEM-NB

C.3.3 RTRV-ALM-ENV (Retrieve-Alarm-Environment)

C.3.3.1 Purpose

The RTRV-ALM-ENV (Retrieve-Alarm-Environment) command instructs the system to retrieve all currently active environment alarms.

C.3.3.2 Input Format

RTRV-ALM-ENV:[tid]::[ctag];

Abortable	Yes
Privilege Code	Reports Only
GSI Confirmation Required	No
File Transfer	No
Related Autonomous Message	None

C.3.3.3 Input Format Parameters

tid Target ID

This parameter appears in the TID Block

Type	String
Required	No
Default Type	Dynamic

Target ID is the name of the system to which the command is addressed.

ctag Correlation Tag

This parameter appears in the CTAG Block

Type	String
Required	No
Default Type	Dynamic

This field is used to associate the command message to the response message.

### C.3.3.4 Output Format

If the command request completes successfully, the following normal completion response is returned:

```
sid date time
AC atag REPT ALM ENV

"AID:NTFCNCDE,ALMTYPE,OCRDAT,OCRTM,ALMSG"
;
```

### C.3.3.5 Output Format Parameters

#### AID Access Identifier

This parameter appears in the Access ID Block

Type	Access ID
Required	Yes

AID is the access identifier of the contact closure.

Expert	English
mc-1-{1-8}	Miscellaneous Contact Closure

#### NTFCNCDE Notification Code

This parameter appears in the Common Block

Type	List
Required	Yes

NTFCNCDE is the alarm level.

Expert	English	Comment
MJ	Major Alarm	
MN	Minor Alarm	
CR	Critical Alarm	

**ALMTYPE****Alarm Type**

This parameter appears in the Common Block

Type	List
Required	Yes

Alarm Type. Use alarm type instead of condition type for RTRV-ALM-ENV.

Expert	English	Comment
ACF	AC Loss (AC Input Power Failure)	
BD	Battery on Discharge	
FAN	Fan Unit Failed	
MISC1	Miscellaneous 1	
MISC2	Miscellaneous 2	
MISC3	Miscellaneous 3	
MISC4	Miscellaneous 4	
MISC5	Miscellaneous 5	
MISC6	Miscellaneous 6	
MISC7	Miscellaneous 7	
MISC8	Miscellaneous 8	
MJF	Fuse Major	
MNF	Fuse Minor	
NONE	None	
PMJ	Power Major	
PMN	Power Minor	
TAMPER	Intrusion (Door Open)	

**OCRDAT****Occurrence Date**

This parameter appears in the Common Block

Type	Date
Required	Yes

This indicates the date of the condition being reported and has the format YY-MM-DD (year-month-day). 70<=yy<=99 maps to 1970 through 1999 respectively; 00<=yy<=37 maps to 2000 through 2037 respectively.

**OCRTM****Occurrence Time**

This parameter appears in the Common Block

Type	Time
Required	Yes

This indicates the time of the condition being reported and has the format HH:MM:SS (hours:minutes:seconds).

**ALMSG****Alarm Message**

This parameter appears in the Common Block

Type	String
Required	Yes
Min # chars	1
Max # chars	40

Alarm Message. Use alarm message instead of condition description. Refer to the Correlation Tables for the default environmental alarm conditions.

**C.3.3.6 Generic Error Responses**

Code	Definition	Reason For Code
CLOS <sup>a</sup>	NE Connection Not Available	Connection with the <NE TID> is not available
IITA	Input, Invalid Target Identifier	TID does not match with SID, has unallowed characters, or string is too long
IICT	Input, Invalid Correlation Tag	Incorrect CTAG
IBNC	Input, Block Not Consistent.	Parameter entered in the wrong block.

<sup>a</sup> only available via AEM-NB

---

# Abbreviations

---

## A

**ADSL**

Asymmetrical Digital Subscriber Line

**AEM-NB**

*AnyMedia™* Access System Element Manager for Narrowband Services

**AFM**

Access Feeder Multiplexer

**AID**

Access Identifier

**AMAS**

AnyMedia Access System

**ANSI**

American National Standards Institute

**AO**

Autonomous Output Message

**AP**

Application Pack

**APOG**

Applications, Planning, and Ordering Guide

**ASCII**

American Standard Code for Information Interchange

**ATM**

Asynchronous Transfer Mode

**AUTO**

Automatic

---

## B

**BAL**

Balance

**BB**

Broadband

**BITS**

Building Integrated Timing Supply

**BRA**

Basic Rate Access

---

## C

### CD

Compact Disk

### CDE

Common Desktop Environment

### CFL

Customer Feature List

### CIT

Craft Interface Terminal

### CIU

Communication Interface Unit

### CLEI

Code assigned by Bellcore

### CO

Central Office

### COBRA

Common Object Request Broker Architecture

### CPE

Customer Premises Equipment

### CR

Critical (alarm severity)

### CRV

Call Reference Value

### CTAG

Correlation Tag

### CTRL

Control

---

## D

### DB

Database

### DC

Direct Current

### DCN

Data Communication Network

### DDS

Digital Data System

### DFL

Default



**DID**

Direct Inward Dial

**DPT**

Dial Pulse Termination

---

**E****ECI**

(Code that corresponds to the bar-coded label on the faceplate of the plug-in)

**EIA**

Electronic Industries Association

**EM**

Element Manager

**ENT**

Enter

**EOC**

Embedded Operations Channel

**EQPT**

Equipment

**ESF**

Extended Super Frame

**ETO**

Equalized Transmission Only

**EVT**

Event

---

**F****FAF**

Facility Failure

**FEF**

Family of Equipment Failure

**FLT**

Fault

**FS**

SuperFrame with Datalink

**FTP**

File Transfer Protocol

**FXO**

Foreign Exchange Office

---

## **G**

### **GSI**

Graphical System Interface

### **GUI**

Graphical User Interface

---

## **H**

### **HDLC**

High Level Data Link Control

### **HP**

Hewlett Packard

### **HW**

Hardware

---

## **I**

### **ICC**

InterChangeability Code

### **ICMS**

Integrated Configuration Management System

### **ID**

Identifier

### **IEEE**

Institute of Electrical and Electronics Engineers

### **IIOIP**

Internet Interoperability Protocol

### **IN**

Information (alarm severity)

### **IP**

Internet Protocol

### **IS**

In Service

### **ISDN**

Integrated Services Digital Network

### **ITU**

International Telecommunication Union

---

## **L**

### **LAN**

Local Area Network

### **LCN**

Local Communication Network

### **LED**

Light Emitting Diode

### **LIC**

License

### **LLN**

Logical Line Number

### **LPBK**

Loop Back

### **LS**

Loop Start

---

## **M**

### **MHz**

Megahertz

### **MJ**

Major (alarm severity)

### **MLT**

Mechanized Loop Testing

### **MM**

Module Manager

### **MN**

Minor (alarm severity)

### **MON**

Degraded Signal

### **MR**

Modification Request

---

## **N**

### **NB**

Narrowband

### **NE**

Network Element

## Abbreviations

---

### **NEM**

Network Element Management / AnyMedia EM subsystem

### **NFS**

Network File Sharing

### **NM**

Network Management

### **NMA**

Network Monitoring and Analysis

### **NMS**

Network Management System

### **NVDS**

Nonvolatile Data Storage

### **NVPS**

Nonvolatile Program Storage

---

## **O**

### **OAM**

Operations, Administration and Maintenance

### **OCU**

Office Channel Unit

### **OMG**

Object Management Group

### **OODB**

Object Oriented Database

### **OOS**

Out Of Service

### **OPS**

Operations System

### **ORB**

Object Request Broker

### **OS**

Operation System

---

## **P**

### **PBX**

Private Branch Exchange

### **PC**

Personal Computer

## Abbreviations

---

**PCM**

Pulse Code Modulation

**PDN**

Public Data Network

**PFU**

Power Filter Unit

**PID**

Password Identifier

**PLL**

Permanent Leased Line

**PLN**

Physical Line Number

**PLR**

Pulse Link Repeater

**POTS**

Plain Old Telephone Service

**PPP**

Point to Point Protocol

**PSTN**

Public Switched Telephone Network

**PT**

Power Test

**PVC**

Permanent Virtual Circuits

---

## R

**RAM**

Random Access Memory

**RCV**

Receive

**RDLD**

Red Lined

**REPT**

Report

**ROC**

Remote Operations Channel

**ROM**

Read Only Memory

**RTU**

Remote Test Unit

---

## **S**

### **SC**

Station Clock

### **SCC**

Serial Communication Channel

### **SCEC**

Secondary Channel Error Correction

### **SCI**

Station Clock Interface

### **SDH**

Synchronous Digital Hierarchy

### **SGE**

Supported Entity Outage

### **SNMP**

Simple Network Management Protocol

### **SPLL**

Semi Permanent Leased Line

### **SVC**

Switched Virtual Circuits

### **SW**

Software

---

## **T**

### **TA**

Terminal Adapter  
Test Area

### **TAP**

Test Access Path  
Test Application Pack

### **TCA**

Threshold Crossing Alert

### **TCP**

Transmission Control Protocol

### **TID**

Target Identifier

### **TL1**

Transaction Language 1

### **TMN**

Telecommunication Management Network

## Abbreviations

---

### **TNM**

Total Network Management

### **TO**

Transmission Only

### **TS**

Test  
Timeslot

---

## **U**

### **UART**

Universal Asynchronous Receiver/Transmitter

### **UAS**

Unassigned

### **UEQ**

Unequipped

### **UI**

User Interface

### **UID**

User Id

### **UPS**

Uninterruptable Power Supply

### **UX**

Unix

---

## **W**

### **WAN**

Wide Area Network

---

## **X**

### **XO**

Crystal Oscillator





---

# Glossary

---

## 10Base T

This is a physical interface used for high speed Ethernet connection. It uses twisted pair cables.

---

## A

### a-wire

One of the two wires of a twisted a/b copper pair. The a/b copper pairs are used for subscriber lines connected for example with Z interfaces, U interfaces or ADSL interfaces. The a-wire is sometimes called tip-wire.

### AEM-NB

*AnyMedia* Access System Element Manager for Narrowband Services. It may be also named simply EM in some parts of the document.

### AID

Access Identifier - AID is the address within a TL1 command that is used to identify the physical or logical entity (or entities) within a network element to which the command applies. It has the format of a unique component identifier followed by hierarchical addresses of components. For example, e1-{1}-{2}-{4} is an object representing E1#4 on IO\_E1 plug-in #2 in *AnyMedia* Access System shelf #1.

### Active plug-in

Identifies the plug-in which is currently responsible for handling the service in a protected configuration. An active plug-in may also be in a state where no service is possible, for example faulty or moved to OOS by the operator.

### ADSL (Full-rate ADSL, Classic)

Asymmetric Digital Subscriber Line - A method of data transmission over unloaded copper loops. The data rate transmitted toward the end user is typically much higher (up to about 6 Mbps) than the data rate transmitted by the end user (up to 640 kbps).

### Alarm

Any condition that needs operator attention, since it may impact the normal operations of any system under operator responsibility (for example Element Manager, Network Element).

### AMS

Alarm Management Subsystem.

### *AnyMedia* Access System

The *AnyMedia* Access System is an access network element (NE) which supports various narrowband and broadband services, digital as well as analog.

### AO

Autonomous output; reports generated by the NEs.

### Apparatus code

The apparatus code is an 8-byte item of ASCII information stored in the nonvolatile data storage (NVDS) of a plug-in (for example LPZ100, DTP500,...). It is a unique identifier which specifies the function of the plug-in.

### Application

Group of one or more modules that offer related functionality.

**Applications Pack (AP)**

This is a circuit pack which provides the line-side interface functionality for POTS, SPOTS, ISDN or special service circuits. Each AP handles 24 or 32 lines (POTS, SPOTS, COIN and special services) or 16 lines (ISDN). There can be up to 16 APs in an *AnyMedia* Access System shelf. APs are for example LPZ100, LPU112, TAP100 as well as ADSL and AFM packs for broadband applications.

**Archive**

Process of copying file systems to removable media (such as tape) and deleting the original files once they have been backed up.

---

## B

**b-wire**

One of the two wires of a twisted a/b copper pair. The a/b copper pairs are used for subscriber lines connected for example with Z interfaces, U interfaces or ADSL interfaces. The b-wire is sometimes called ring-wire.

**Backup**

Process of copying file systems to removable media (such as tape) to safeguard against loss, damage, or corruption.

**BB**

Broadband.

**BCC protocol**

Bearer Channel Connection protocol - This is a V5.2 protocol which allocates bearer channels on demand.

**Bearer channel**

A 64-kbps timeslot within the V5.x interface allocated for a B-channel of an ISDN user port or a channel from a POTS user port.

**Blinking Alarm**

An alarm which is continuously changing its status: raised, clear, raised, clear ...

**Bridge**

A network layer device that passes packets between two or more network segments that use the same data link communications protocol (OSI layer 2). The network segments appear as one segment to protocol levels higher than the data link layer. The bridge recognizes with the help of the MAC address which LAN component is connected at which port of the bridge. Data packets are only transferred over the bridge if the participant is at another port of the bridge. With a bridge, data traffic can be kept from a certain part of a LAN.

**Built-in Self Test (BIST)**

This is a procedure executed by each plug-in circuit pack either after power-up or on demand. The task is to check the functions of the hardware.

**Burst Load**

Load that can occur in certain well-known circumstances, where response times are no longer guaranteed, but queues handle excess traffic. After removing the causes of the burst load, and a certain settling time, normal operation is resumed. During burst load there is a graceful degradation, no loss of information, only a queueing occurs to defer the load to a later moment.

**Busy Hour Load**

Maximum load that is expected to occur in real life that must be handled with normal response times.

---

## C

### **Circuit**

This refers to the devices and functions built on or provided by an AP for one port. In some documents this is also called facility. The subscriber line is not included.

### **CIT: Craft Interface Terminal**

A local RS232 connection on the *AnyMedia* access system to which a PC GUI can be connected.

### **Client**

An entity that initiates requests to a server. For the *AnyMedia* Access System a client could be a PC with a GUI interface, a telnet session or an OS (like the AEM-NB).

### **Client Application**

A group of one or more user modules that offer related functionality.

### **Client Host**

A machine where one or more user modules are installed.

### **Common Data and Control Pack (COMDAC)**

Common Data and Control - Plug-in which provides the central control and transmission fabric for the *AnyMedia* Access System. The COMDAC supports multiple system applications, including V5.x switched services and analog and digital leased lines (ALL and DLL) and a variety of application packs.

### **Communication channel**

A group of one or more communication paths, all of different types. Is associated to a 64-kbps timeslot on a V5.x interface. This association may be changed by a protection switch (only V5.2).

### **Communication path**

A communication path carries any one of the following information types:

- layer 2 data links carrying the control protocol, link control protocol, PSTN protocol, protection protocol and BCC protocol,
- all the ISDN Ds-type data (ISDND) (signaling), ISDN p-type data (ISDNP) and ISDN f-type data (ISDNF) from one or more user ports.

It should be noted that this definition includes the possibility that there is more than one communication path of the same information type, each allocated to a different logical communication channel.

### **Configuration Management**

This consists of a set of functions for controlling the network elements, including initialization, parameter setting, starting and stopping and collecting information about the NE configuration.

### **Cross-Connection**

A term for a logical association between two objects, e.g. between a subscriber port and a network interface. A physical cross-connection may additionally be established in the case of a network interface where bandwidth allocation is done on a provisioning basis (V5.1). In the case of V5.2 the bearer channel allocation is done on a per-call basis by the BCC protocol.

---

## D

### **Date**

This refers to the day, month, and year and represents a calendar function that needs to include a calculation for leap years and a capability of determining the day of the week from the date, and must be Y2K compliant.

**DCN**

Data Communications Network; the communication media and interconnected devices used to exchange management information between the AEM-NB, the NEs and other OSs.

**Defaults**

Defaults are the parameter values built into the *AnyMedia* Access System when it is shipped from the factory. The sum of all defaults forms the default configuration. (Default values are restored upon execution of an Initialize-System command.) For TL1 commands there are defined defaults for parameter values which are used for parameters not given in the command line.

**Device Driver**

A program that controls a specific device, such as a cartridge tape (DAT).

**Distribution Port**

The circuitry that provides narrowband access (i.e., up to the 1.544 Mbps DS1 rate) to a single network interface over one (2- or 4-wire) metallic facility and converts between the format seen by this network interface (e.g., analog voice-frequency, ISDN U-interface, etc.) and the internal format (i.e., 4-Mbps timeslots). Distribution Ports are contained in Application Packs / Channel Units for the *AnyMedia* Access System. A maximum of 32 Distribution Ports are supported on POTS/COIN Application Packs (APs) and a maximum of 16 Distribution Ports are supported on ISDN APs.

**Download**

The process of moving information from a server to a client at the request of a client according to client/server paradigm. Expected applications of this capability are database retrievals.

**Drop**

This comprises the wire to the customer and customer premises equipment (CPE). In some documents this is also called equipment.

**Duplex mode**

Two COMDACs are equipped in the *AnyMedia* Access System. One COMDAC is active and controls the whole system, the other is in stand-by mode. During operation the memories (NVPS, NVDS and RAM) of both are mutually consistent. One reason to perform a side switch is if the active COMDAC fails. In this case the COMDAC previously in stand-by mode is now active.

---

**E****E1**

E1 is the standard acronym for the 2.048-Mbit/s interface defined in the ITU-T Recommendations G.703/G.704.

**EAS Element Access Server**

This is a CORBA server developed by Lumos Technologies which provides an interface between TL1 messages and CORBA methods.

**EM Domain**

An assigned collection of Controlled Objects.

**EM Task**

This represents a subset of the management functions supported by EM applications.

**EM User**

An entity defined via login name that can be assigned at least to an AEM-NB user group.

**EM User Group**

A logical group of EM users enabled to access one or more "domains". Permissions to access domains, applications and tasks are administered on an EM user group basis.

**Embedded Operations Channel (EOC)**

A duplicated DS0 data link dedicated for exchange operations messages between the LDS and RDT.

**Entity**

The term entity or object represents an entry in a TL1 administrative view, i.e. an entity (or object) may be entered, changed, deleted or retrieved by a TL1 command.

---

**F****Far end**

Any other network element residing in the network complex away from the AEM-NB (that is the location of the service node is at the opposite end of the feeder E1 for the reported failure).

**Fault Case**

For some faults (e.g. DCN failure), normal working conditions need to be re-established within certain time limits. These are fault cases that are taken into account.

**Fault Management**

For detecting, displaying, storing, filtering and routing fault/alarm data.

**Flag monitoring**

The flag monitoring function requires that flags, sent on V5 communication channels towards the NE by the LE, must be monitored in the NE. Flag monitoring is mandatory for V5.2 interfaces and optional for V5.1 interfaces; flag sending is mandatory in any case for both directions, i.e. NE to LE and LE to NE.

**Forced Switch**

This refers to an Element Manager-initiated switch command that instructs the NE to perform a switch no matter what the conditions of the protection unit (COMDAC and IO\_HDLC circuit packs only) are.

**Full Backup**

This copies a complete file system or directory.

---

**G****General settings**

These are parameters which are valid for all customer-specific configurations (for example loop-start function for all Z ports which are assigned for POTS service or suppression of out-band signalings for Z ports which are assigned for ALL (transmission-only) service).

**GSI**

Graphical System Interface - A user-friendly front-end for communicating with a system. In the *AnyMedia* Access System the GSI is installed on a Windows 95 personal computer and used for entering and receiving TL1 (Transaction Language 1) messages. The GSI provides support for managing the *AnyMedia* Access System in the following functional areas:

- Configuration management
- Fault management
- Performance management
- Security management
- Inventory management.

**GSI-NB**

The Graphical System Interface for narrowband services. This is a Windows 95-based PC which uses TL1 commands for the management of *AnyMedia* Network Elements.

## GUI

The Graphical User Interface of the AEM-NB.

---

## H

### Host

A machine where one or more modules are installed.

### Hub or Multiport Repeaters

This have 8, 12, 16 or more ports. With their help multiple devices with 10BASE-T interface can be connected to a single LAN. They have at least one additional port for connecting an additional segment of a LAN.

---

## I

### Incremental Backup

This copies new files and files that have changed since a previous backup. The incremental backups are usually given a dump level which determines which files are backed up. A certain level incremental backup will save all the new or changed files since the last backup with a lower level.

### Inhibit Switch

This refers to an Element Manager-initiated switch command that instructs the NE to inhibit a side switch irrespective of the conditions of the active unit (COMDAC and IO\_DS1 circuit packs only).

### Internationalization

This is the process of isolating the language- and customs-dependent code in a computer program from the language-independent code. The term internationalization is often abbreviated as *i18n*.

### IP Addresses

These are distributed according to the worldwide or local configuration. The IP address is used in ISO layer 3. A LAN contains tables for making an assignment between MAC address and IP address.

### INIT-SYS command

The INIT-SYS command is used to clear the database and to restore the *AnyMedia* Access System to default values set at factory.

### Inventory

The inventory is the summary of data stored on a plug-in in the NVDS during manufacturing which is used to identify the plug-in and its functionality.

### ISDN BRA service

Integrated Services Digital Network Basic Rate Access Service - Connects ISDN BRA subscribers to the network via dial up connection.

---

## L

### Level 1 Applications

The minimum set of server applications that have to run together to provide the minimum functionality of the AEM-NB. These applications must exist before the Level 2 Application can be started. If this group is shut down the AEM-NB is shut down.

**Level 2 Applications**

Server applications that can be started up and shut down individually without affecting the functioning of other applications.

**Line Test**

Also called drop test. This checks for open circuits, short circuits, leakages to ground, foreign voltages, or other faults on the subscriber line that connects an AP port circuit to the CPE. The results are used to detect broken or bad quality wires even before the customer realizes a lack of quality.

**LL/PLL Permanent Leased Lines**

A service in which resources are used permanently for the transmission of data between two points. The switch is not responsible for setting up this service.

**Locale**

This is a geographic or political region that shares the same language and customs. In this document, a locale is also used to refer to the definition of the subset of a user's information technology environment that depends on language and cultural conventions.

**Localization**

This is the process of adapting a program for use in a specific locale.

**LOG File**

This is the file used for listing all actions that have occurred in a system. This information is generated and recorded concurrently and sequentially as transactions and events are processed in the system.

**Logical line identity**

For logical addressing of an end-customer termination either associated to a V5.1 or a V5.2 interface

**Logical link**

A logical entity providing 31 64-kbps timeslots which is associated to a 2.048-Mbps interface. One (V5.1) or more links (only V5.2) may be related to a V5.x interface.

---

## M

**MAC Address**

This is a 6-byte hardware address, which identifies a unique participant worldwide in an Ethernet LAN. A MAC address is used in OSI layer 2.

**Manual (normal) Switch**

This refers to an Element Manager-initiated switch command that instructs the NE to perform a switch only if the protection unit (COMDAC and IO\_HDLC circuit packs only) is in service and not faulty.

**Migration**

This refers to converting an NE from one software release to another by installing a different software release.

**Mixed ISDN/POTS mode**

An operation mode of the *AnyMedia* Access System where ISDN and POTS service is possible. Because ISDN subscribers are provisioned, the frame relay function has to be performed. Therefore at least one IO\_HDLC plug-in is necessary (optionally a second one for protection). V5 communication channel information is frame relayed on the IO\_HDLC plug-in and routed towards ISDN subscribers (for ISDN D-channel information) and to the COMDAC (for V5 layer 3 protocols) respectively.

**Module**

An executable installed on a Host.

---

## N

### NE

*AnyMedia* Access System Network Element.

### Non-Volatile Data Storage (NVDS)

This refers to a capability of the *AnyMedia* Access System to store information in such a way as to survive indefinite periods of total power failure. The current values for all provisionable parameters are stored in the NVDS and hence are the parameter values that will be used on subsequent NE power-up.

### Non-revertive mode

A certain system resource which has become faulty and thus caused a switch to or a replacement by a certain other (standby) resource is NOT reused automatically if the (temporarily) faulty resource returns back to operation. Instead of this the standby resource is used furtheron. A switch back may take place later on, but is independent from the recovery of the (temporarily) faulty resource.

Examples:

- a) If a reference clock switch between COMDAC phase locked loop (PLL) reference clock inputs has occurred due to a failure condition, the AEM-NB will not automatically return to the primary reference, even if the failure condition has cleared.
- b) V5.2 protection switching of communication channels.

### Non-Volatile Program Storage (NVPS)

This keeps software program data. It resides in the COMDAC.

### Normal Hour Load

The average load expected during the lifetime of the system.

### NVDS

Nonvolatile Data Storage - NVDS refers to that part of the database which can be retained even after a power failure, for example provision parameters.

### NVPS

Nonvolatile Program Storage - NVPS refers to nonvolatile memory on the COMDAC used to store the load image.

---

## O

### Off-line Backups

These are backups performed automatically via any scheduling mechanisms, e.g. cron file.

### On-line Backups

These are backups performed on user demand.

### Operator

This refers to the *AnyMedia* Element Manager users.

### Operator Mode

Testing initiated by staff from the EM using the NE-integrated capabilities. These tests can last some time, e.g., some measurements can be executed several times during a test session. The results in this mode usually are values (e.g. resistance, voltage, ...) and pass/fail decisions.

### Overload

The load that causes the system to take drastic measures to ensure its integrity. During overload normal system function is disrupted and certain inputs (the ones causing the overload) are ignored. After clearing the overload situation, the system is left in asynchronous state for those inputs that generated the overload. Re-synchronization of this input retrieves synchronization.



## OS

This is any operations system or Element Manager connected to the *AnyMedia* Access System by some means of communication. For the AEM-NB the communication method is TCP/IP.

---

## P

### Password (PID)

Character string used to authenticate the identity of a user. The password should consist of 6 to 10 case sensitive alphanumeric characters, it should be changed frequently, it is stored and transmitted in an encrypted form.

### PCM Highway

The COMDAC pack is connected to each AP by the PCM highway, which consists of two 4.096-Mbps serial links, a 4.096-MHz clock and an 8-kHz sync signal. The *AnyMedia* Access System uses two PCM highways between the COMDAC, the IO\_HDLC and each of the 16 AP slots.

### Performance Management

For receiving, detecting, time stamping, analyzing, displaying and storing performance data.

### Plain Old Telephone Service (POTS)

The conversational 2-wire analog subscriber service.

### Platform

The hardware on which any *AnyMedia* EM module, server or client, is running.

### Platform Alarm

This is an alarm related to the *AnyMedia* Element Manager application or its hardware/software platform. It usually refers to an Element Manager function or hardware/software platform object.

### PLL

Permanent Leased Line - These lines may be analog (ALL) or digital (DLL). They are not switched services and are not carried to the LE through the V5 interface but on special separate 2-Mbps links.

### Plug-in

Term that is generally used for circuit pack units (for example LPZ100, IO\_E1 ) which have pre-designated slots with the capability to plug in the circuit pack. Channel units are a subset of circuit packs used for supporting specific telephony functionality as in the case of line termination plug-in.

### Port

This is circuitry built on an AP to provide an interface for subscribers. Note that more than one port can be housed on an AP, e.g. the LPZ100 provides 32 Z-ports.

### Port Test

Also called circuit test. Verifies the ability of an AP port to provide proper transmission and signaling. It is the testing of the port hardware. The functions of the port test rather depend on the hardware function of the circuit (e.g. POTS, pulse metering, ISDN, ...). These tests are performed on each AP using part of their self-test capabilities.

### Primary link

The 2.048-Mbps link in a multi-link V5.2 interface whose physical communication channel in timeslot 16 carries a communication path for the protection protocol and, on V5.2 initialization, also the communication path for the control protocol, link control protocol, and the BCC protocol. Other communication paths may also be carried in the timeslot 16.

### Protection group 1

This is the standard group of physical communication channels consisting of the protected logical communication channel on the primary link and the protecting standby channel on the secondary link of a V5.2 interface, each located in timeslot 16.

**Protection group 2**

This is an optional protection group of a V5.2 interface, consisting of up to 3 standby communication channels, serving as protecting channels for all logical communication channels, not included in protection group 1.

**Protection switch**

A switch of the service from the service plug-in to the protection plug-in. A protection switch can be requested manually or driven by plug-in fault.

**PSTN (user port)**

Public Switched Telephone Network - Delivers analog telephony and data services to a POTS subscriber. It is addressed by a logical layer 3 address used in the relevant protocols on the V5.x interface. With respect to the V5.x interface the layer 3 address uniquely identifies one PSTN user port.

---

## R

**Response Time**

The real elapsed time between detectable start of an action and its completion.

**Restore**

The process of copying backup files from removable media to a working directory, replacing the original files which could have been damaged.

**ROC (Remote Operations Channel)**

The bearer channel that conveys management information for a remote system (*AnyMedia* NE). The ROC is intended to be used when the system is installed at locations where no local Ethernet LAN and no separate network (e.g., X.25) exists.

**Router**

A network layer device that forwards packets from one network to another based on network layer information (OSI layer 3). Data packets are only transferred through the router if the participant is connected to another port of the router. With a router, data traffic can be kept from certain parts of a LAN. A router is more powerful than a bridge, it reduces the traffic on a LAN more than a bridge, because the IP address is evaluated for traffic control.

---

## S

**Station Clock**

An external 2048 kHz synchronization signal, according to ITU-T G.703.

**Security Management**

This restricts access based upon the establishment of log-in procedures and an associated set of passwords. Screen locks are used as well.

User access is based upon domain partitioning. Controls the access to the data and capabilities inherent within a fixed partition of the network, including unbundling.

**Server**

A network element that waits for requests from clients to perform specific tasks. This is the function performed by the *AnyMedia* Access System.

**Server Application**

This is a set of server processes that perform a certain function.

**Server Host**

This is the machine where the system server modules are installed.

**Server Module**

This is the module that provides a subset of the system services.

**Service**

This is a piece of functionality provided by a server module.

**Service State (of an object or entity)**

This represents the current availability status of an associated resource or service in the NE from the management point of view (e.g., memory administration, maintenance).

**Side Switching**

This refers to the operation of deactivating the active core entity and activating the standby core entity (COMDAC and IO\_HDLC circuit packs).

**Simplex mode**

One COMDAC is equipped in the *AnyMedia* Access System and controls the whole system. If this COMDAC fails the system also fails.

**Software Download**

The transport of the information required to upgrade/update a given NE's generic program.

**Software package**

At the architectural level, software packages are the primary vehicle for functional partitioning of the system. Software packages are configuration units of the system.

**SPLL: Semi Permanent Leased Lines**

A service in which resources are used permanently for the transmission of data between two points. The switch is responsible for setting up this service.

**System**

AEM-NB software. It provides a set of services allowing an operator to manage the *AnyMedia* NE.

**System Failure**

Any problem that prevents the AEM-NB from continuing to work.

---

## T

**TAS (Terminal Access Server)**

This adapts local area networks (LAN) to wide area networks (WAN). TASs have the ability to integrate remote network elements in a local network. TASs support different LAN protocols (e.g. Ethernet) and WAN protocols (e.g. PPP).

**TCA (Threshold Crossing Alert)**

A crossing of a parameter threshold that is generally considered to be a transient condition.

**TAP100**

Test Application Pack - TAP100 is the internal test head executing the measurements required for the drop.

**TELNET**

This is a remote terminal interface protocol which allows remote login capability into a system on a network from any other node on that network that is also running TELNET. TELNET is a TCP/IP application.

**Test Access Path (TAP)**

There are up to two TAPs, one consisting of two pairs (TAP-B) and the other of six pairs (TAP-A), both providing internal and external metallic test access to the circuits.

**Test Session**

This is the procedure including all necessary functions to test a subscriber. This includes the setup of the test path as well as the release of the test equipment. The test session runs in the NE.

**Time**

This represents a 24-hour clock function.

**TL1 (Transaction Language 1)**

This is a bellcore standard message language. It is the primary means of operating and maintaining the V5DLC system. A TL1 message session supports bi-directional message transmission and when a TL1 link is established, the system can initiate autonomous messages to monitor alarms and changes in system status.

**TS**

Timeslot - Any cyclic time interval that can be recognized and defined uniquely. For example a 64-kbps channel of a V5 interface that can be used either as a bearer channel (carrying subscriber payload information) or as a communication channel (carrying both subscriber and network element signaling information).

---

## U

**Upgrade**

Is a type of migration where the software release is changed from an earlier release to a later release.

**Upload**

The process of moving information from a client to a server at the request of a client according to client/server paradigm. Intended applications of this capability are software updates and restoring databases.

**User**

The operator who will use the EM to provision, maintain and monitor the *AnyMedia* Access System.

**User Identifier (UID)**

This is a unique user login identifier. This string is required and cannot be null. Grouping of UID string values for this command is not allowed. The valid UID value is a 3 to 10 case-sensitive alphanumeric character string.

---

## V

**V5.x interface**

An ETSI defined interface between a local exchange and an access network element. A V5.1 interface consists of one single 2-Mbps (E1) link containing communication channels and bearer channels. A V5.2 interface consists of up to sixteen 2-Mbps (E1) links containing communication channels and bearer channels. The term V5.x interface is used for clarification that certain facts, a certain description or requirements are relevant for both V5.1 and V5.2 interface.

---

## W

**Workload or Load**

A mix of actions and their frequencies from all possible input points that need processing in some way in the system.

---

## Z

### **Z-port**

A Z-port is circuitry built on a POTS AP to provide a Z interface for analog subscribers. Note that more than one Z port is housed on an *AnyMedia* Access System POTS AP, for example the LPZ100 provides 32 Z-ports.

### **Z-port (for transmission only)**

This is a Z-interface normally used for services other than telephony (e.g. data transmission). This type of Z-interface does not support DC feeding and does not support out-band signaling. This interface can support Analog Leased Line (ALL) service.



---

# Index

---

## A

Access bar [3-4](#)  
Access protection [1-27](#)  
Access to the testroutines [6-23](#)  
Actions [1-13](#) [3-31](#)  
AEM external system LAN interface [A-5](#)  
AEM-NB protocol profiles [A-5](#)  
Alarm  
    ~ log [1-24](#)  
    ~ monitoring [1-22](#)  
    Classification [6-44](#)  
Alarm counter [3-4](#)  
Alarm cut-off function (ACO) [5-4](#)  
Alarm data synchronization [6-42](#)  
Alarm interfaces  
    Miscellaneous alarm closure inputs [5-4](#)  
    Office alarm interfaces [5-4](#)  
Alarm management [3-18](#)  
Alarm Notification icon [3-4](#)  
Alarm Reporting [6-3](#)  
Alarm Severities [6-45](#)  
Alarm Viewer  
    Alarm Table [6-15](#)  
    General Information [6-14](#)  
    Menu Bar [6-12](#)  
    System management functions [6-18](#)  
    Toolbar [6-14](#)  
Alarm viewer  
    Starting [6-10](#)  
Alarms  
    Alarm classification [6-44](#)  
    Reporting via EM [6-3](#)  
Alternate key [3-6](#)  
AnyMedia Access System  
    overview [5-1](#)  
AP provisioning [5-39](#)  
Applications, start [3-4](#)  
Apply (button) [3-15](#)  
Archive (database) [3-23](#)  
Archive command [3-26](#)  
Assign  
    ~ controlled objects to domains [4-13](#)  
    ~ user groups access to applications [4-25](#)  
    ~ user groups access to domains [4-24](#)  
    ~ user groups access to tasks [4-26](#)  
    ~ users to user groups [4-6](#)  
Association (NE-AEM) [6-43](#)  
Association state [6-43](#)  
Authentication [5-20](#)

Autonomous Reports [1-13](#) [3-31](#)  
Available Domains [5-19](#)

---

## B

Backspace key [3-6](#)  
Backup  
    ~ command [3-25](#)  
    ~ level [3-28](#)  
    ~ schedules [3-28](#)  
    ~ types [3-24](#)  
Backup (database) [3-23](#)  
Bridge (definition) [A-2](#)  
Built-in self-test [6-32](#)  
Buttons, often used  
    Apply [3-15](#)  
    Cancel [3-15](#)  
    Close [3-15](#)  
    OK [3-15](#)

---

## C

Cancel (button) [3-15](#)  
CDC test result [6-37](#)  
CD-ROM [XIX](#)  
Check box [3-14](#)  
CIT port protocol profiles [A-3](#)  
Click (mouse) [3-6](#)  
Client application [3-17](#)  
Close (button) [3-15](#)  
COMDAC protection mode (simplex) [5-58](#) [5-60](#)  
COMDAC Protection State [5-59](#)  
Comments on document [XX](#)  
Communications Info [5-20](#)  
Configuration data synchronization [6-41](#)  
Configuration Management [1-3](#)  
Configuration management [3-18](#)  
Connection State [5-20](#)  
Connection states (NE-AEM) [6-40](#)  
Control key [3-6](#)  
Controlled Objects [4-29](#)  
Core application [3-17](#)  
Craft interface terminal [A-2](#)  
Create  
    ~ domain [4-8](#)  
    ~ user [4-2](#)  
    ~ user group [4-16](#)  
Cross-connection  
    General [5-78](#)  
cross-connections [5-79](#)  
Cursor aspects [3-7](#)  
Cursor menu [3-11](#)

cursor menu [5-8](#)

---

## D

Data Communications Network (definition) [A-2](#)

### Database

- Archive [3-23](#)
- Backup [3-23](#)
- Full backup [3-23](#)
- Incremental backup [3-24](#)
- Off-line backup [3-24](#)
- On-line backup [3-24](#)
- Restore [3-23](#)

DCN configurations [A-5](#)

DCN introduction [A-1](#)

Deinstall AEM [3-20](#)

Deinstallation commands [3-20](#)

### Delete

- ~ domain [4-14](#)
- ~ user [4-6](#)
- ~ user group [4-26](#)

Delete key [3-6](#)

disk space [2-2](#)

Documentation [XVIII](#)

- Comment procedure [XX](#)
- Packaging and format [XVIII](#)

### Domain

- Create ~ [4-8](#)
- Delete ~ [4-14](#)
- Modify ~ [4-11](#)

Double click (mouse) [3-6](#)

Drag (mouse) [3-6](#)

Drop-down list box [3-15](#)

---

## E

Environment Alarms [6-44](#)

Escape key [3-6](#)

External LAN AEM system interface [A-5](#)

External LAN interface profiles [A-3](#)

External system LAN interface [A-3](#)

---

## F

### Fault

- clearance [1-24](#)
- identification [1-23](#)
- source [1-24](#)

Fault Management [1-3](#)

---

### File

Close [6-12](#) [6-18](#)

Exit [6-12](#) [6-18](#)

New [6-12](#) [6-18](#)

Print [6-12](#) [6-18](#)

Reload [6-13](#) [6-18](#)

Full backup (database) [3-23](#)

Functional diagram

Cross-connections [5-78](#)

---

## H

Help icon [3-5](#)

Help Installation [2-34](#)

---

## I

Icon [3-8](#)

Icons, greyed [3-4](#)

Incremental backup (database) [3-24](#)

Input focus [3-7](#)

### Installation

third-party software [1-20](#)

integrated management mode [1-5](#)

### Interfaces

Synchronization interfaces [5-3](#)

Inventory Management [5-6](#)

IP Address [5-20](#)

---

## J

jre Installation [2-29](#)

---

## K

Keyboard [3-6](#)

### Keys, special

Alternate [3-6](#)

Backspace [3-6](#)

Control [3-6](#)

Delete [3-6](#)

Escape [3-6](#)

Return [3-6](#)

---



---

## L

LAN interface, external system [A-3](#)  
Level 1 application [3-17](#)  
Life cycles  
    network [1-19](#)  
List box [3-15](#)  
Log  
    alarm ~ [1-24](#)  
Log alarms [3-32](#)  
Log management [3-31](#)  
Log out (workspace menu) [3-13](#)  
Log shortening [3-32](#)  
Log size [3-31](#)  
Log type  
    Actions [1-13](#) [3-31](#)  
    Autonomous Reports [1-13](#) [3-31](#)  
    System Internal Events [1-13](#) [3-31](#)  
Log Viewer application [3-32](#)  
LOG\_DEL\_FULL [6-46](#)  
LOG\_DEL\_PART [6-47](#)  
Login [3-2](#) [5-20](#)  
Logout  
    ~ manually from System [3-3](#)  
Loopback  
    Clear [6-38](#)  
    Set [6-38](#)  
    Test [6-37](#)  
LUMOS Installation [2-9](#)

---

## M

Menu  
    Actions [6-13](#)  
    File [6-12](#) [6-18](#)  
    Filters [6-13](#) [6-19](#)  
    Help [6-14](#)  
    Options [6-13](#)  
    Views [6-13](#)  
Menu bar [3-11](#)  
Menus, often used  
    File -> Exit [3-16](#)  
    File -> Print [3-16](#)  
    Help -> Index [3-16](#)  
    Help -> On Window [3-16](#)  
Metallic Shelf Controller [2-2](#)  
Minimize/Restore Front Panel (workspace menu) [3-13](#)  
Miscellaneous alarm closure inputs [5-4](#)  
Modifying  
    network [1-25](#)  
    network element [1-26](#)  
Mouse [3-6](#)

---

## N

NE Date & Time [5-56](#)  
NE Details [5-18](#)  
NE id [5-18](#)  
NE Memory Administration [5-6](#)  
NE Software Administration [5-6](#)  
NE\_ASSOC\_FAILED [6-47](#)  
NE-AM Alarms [6-44](#)  
NEASSOC\_LOST [6-48](#)  
Netscape Installation [2-32](#)  
Network  
    life cycle [1-19](#)  
    modifying [1-25](#)  
    normal operation [1-22](#)  
    physical installation [1-20](#)  
Network Browser [5-8](#)  
Network element  
    modifying [1-26](#)  
    registration [1-21](#)  
Network element management [3-18](#)  
Network planning [1-20](#)  
Normal Alarms [6-44](#)  
NVDS  
    Data Backup [5-71](#)  
    Data Restore [5-72](#)

---

## O

ObjectStore Configuration [2-20](#)  
ObjectStore Installation [2-19](#)  
Office alarm interfaces [5-4](#)  
Off-line backup (database) [3-24](#)  
OK (button) [3-15](#)  
On-line backup (database) [3-24](#)  
Option menu [3-15](#)  
OrbixMT Installation [2-12](#)  
OrbixNames Installation [2-14](#)  
OrbixTalk Installation [2-15](#)  
OrbixWeb Installation [2-30](#)  
Ordering  
    Document [XIX](#)

---

## P

Pass-through interface [C-1](#)  
Password [5-20](#)  
Path-through interface, TL1 messages [C-3](#)  
Performance  
    ~ monitoring [1-26](#)

Performance Management [1-4](#)  
Periodical Alarm Deletion [6-9](#)  
Platform Alarm [6-44](#)  
Plug-in unit  
    adding [1-26](#)  
    removing [1-26](#)  
Port test [6-29](#)  
Port test result [6-27](#) [6-30](#)  
Print reports [3-21](#)  
Product safety  
    Classification [XVII](#)  
Programs (workspace menu) [3-13](#)  
protection  
    forced switching [5-60](#)  
    inhibit switching [5-60](#)  
    manual switching [5-60](#)  
    side switching [5-60](#)  
Protection Switching  
    COMDAC [5-60](#) [5-62](#)  
    HDLC [5-63](#)  
Provisioning  
    network [1-21](#)  
Pushbutton [3-14](#)

---

## Q

Quitting the Alarm Viewer [6-11](#)

---

## R

Radio button [3-15](#)  
Reaction  
    to fault identification [1-24](#)  
Recovery [1-24](#)  
Refresh (workspace menu) [3-13](#)  
Remote Operations Channel (definition) [A-2](#)  
Remote Operations Channel protocol profiles [A-4](#)  
Remote Operations Channel, protocol [A-4](#)  
Repetitive Alarm [6-7](#)  
Restart Workspace Manager (workspace menu) [3-13](#)  
Restore (database) [3-23](#)  
Restore command [3-26](#)  
Return key [3-6](#)  
RogueWave Installation [2-10](#)  
Router (definition) [A-2](#)

---

## S

Safety  
    Classification [XVII](#)

SCHED-EX [6-31](#)  
Screen navigation  
    equipment configuration [5-14](#)  
Security Management [1-4](#)  
Selected Domains [5-19](#)  
Server application  
    Definition [3-17](#)  
    restart [3-18](#)  
    shut-down [3-19](#)  
    start options [3-17](#)  
    start-up [3-19](#)  
Server applications  
    Alarm management [3-18](#)  
    Configuration management [3-18](#)  
    Network element management [3-18](#)  
    System core [3-18](#)  
Server applications of AEM [3-18](#)  
Server applications start-up via a command line [3-20](#)  
Shelf Layout [5-3](#)  
Shelf protection  
    COMDAC [5-60](#)  
Shelf view [5-22](#)  
Shuffle Up/Down (workspace menu) [3-13](#)  
Software  
    ~ installation [1-20](#)  
    copy [5-69](#)  
    download [5-65](#)  
    upgrade [5-65](#)  
Software packages [2-3](#)  
Software packages dependencies [2-40](#)  
Sorting Alarms [6-17](#)  
Spin box [3-15](#)  
screen navigation  
    service provisioning [5-80](#)  
stand-alone mode [1-5](#)  
Standby card test scheduling [6-31](#)  
Status Bar [5-8](#) [5-11](#)  
Status bar  
    Message area [5-11](#)  
    Progress area [5-11](#)  
    Stop / Cancel button [5-11](#)  
Supported Interfaces [5-77](#)  
SWVR\_ILLEGAL [6-49](#)  
Synchronization  
    alarm data [6-42](#)  
    configuration data [6-41](#)  
System  
    ~ security [1-27](#)  
System Administration application [3-18](#)  
System core [3-18](#)  
System Internal Events [1-13](#) [3-31](#)  
System management functions [6-18](#)

## T

Tab [3-15](#)  
 TAP test result [6-34](#)  
 Target ID [5-20](#)  
 TCP/IP\_CON\_REFUSED [6-49](#)  
 Terminating the Alarm Viewer [6-11](#)  
 Testing interfaces [5-4](#)  
 Testroutines  
   Access to the ~ [6-23](#)  
   Built-in self-test [6-32](#)  
   Loopback test [6-37](#)  
   Port test [6-29](#)  
   Port test result [6-27](#) [6-30](#)  
   Result of standby card test scheduling [6-32](#)  
   Standby card test scheduling [6-31](#)  
   TAP test result [6-34](#)  
 Text box [3-15](#)  
 timing source [5-52](#)  
 timing source control  
   primary source [5-54](#)  
   secondary source [5-54](#)  
   timing sync mode [5-54](#)  
 TL1 messages (Path-through interface) [C-3](#)  
 TL1\_COMM\_DENIED [6-50](#)  
 Trademarks [XIV](#)  
 TST-ANALG [6-29](#)  
 Typographical conventions [XV](#)

## U

Unassign  
   ~ controlled objects from domains [4-13](#)  
   ~ user groups access from applications [4-25](#)  
   ~ user groups access from domains [4-24](#)  
   ~ user groups access from tasks [4-26](#)  
   ~ users from user groups [4-6](#)  
 User  
   Create ~ [4-2](#)  
   Delete ~ [4-6](#)  
   Modify ~ [4-4](#)  
 User administration [4-1](#)  
 User group  
   Create ~ [4-16](#)  
   Delete ~ [4-26](#)  
   Modify ~ [4-21](#)

## V

V5 Interfaces [5-83](#)

V5 Protocol [5-79](#)

## W

Window controls [3-7](#) [3-8](#)  
   maximize button [3-9](#)  
   menu bar [3-9](#)  
   minimize button [3-8](#)  
   scroll bar [3-9](#)  
   title bar [3-8](#)  
   window frame [3-8](#)  
   window menu [3-9](#)  
 Window controls, AEM-NB windows [3-13](#)  
 Window menu [3-10](#)  
   Close [3-10](#)  
   Lower [3-10](#)  
   Maximize [3-10](#)  
   Minimize [3-10](#)  
   Move [3-10](#)  
   Restore [3-10](#)  
   Size [3-10](#)  
 Windows, basics [3-7](#)  
 Workspace manager [3-12](#)  
 Workspace menu [3-12](#)  
   Log out [3-13](#)  
   Minimize/Restore Front Panel [3-13](#)  
   Programs [3-13](#)  
   Refresh [3-13](#)  
   Restart Workspace Manager [3-13](#)  
   Shuffle Up/Down [3-13](#)

